

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22

U.S. DEPARTMENT OF HOMELAND SECURITY

WASHINGTON, D.C.

- - -

GOVERNMENT 2.0: PRIVACY AND BEST PRACTICES

THE WASHINGTON COURT HOTEL, ATRIUM BALLROOM

525 NEW JERSEY AVENUE, N.W.

WASHINGTON, D.C.

- - -

JUNE 22, 2009

MODERATORS

MR. PETER SAND, PANEL 1

MS. MARTHA K. LANDESBURG, PANEL 2

MR. EARL CRANE, PANEL 3

WELCOME ADDRESS

MARY ELLEN CALLAHAN, Chief Privacy Officer, DHS

1 OPENING REMARKS

2 VIVEK KUNDRA, Federal Chief Information Officer

3

4 PANELISTS:

5 MAXINE TELLER

6 VICTOR E. RICHE

7 JODI CRAMER

8 LENA TRUDEAU

9 BOB BURNS

10 JEREMY AMES

11 JONATHAN CANTOR

12 DANIELLE CITRON

13 LILLIE CONEY

14 TIM JONES

15 JAY STANLEY

16 HEATHER WEST

17 BRIAN BURNS

18 DAN CHENOK

19 MARK DRAPEAU

20 EDWARD W. FELTEN

21

22

1 WELCOME ADDRESS:

2 MS. LEVIN: Good morning. I think we're ready to
3 begin, key people have arrived. My name is Toby Levin
4 and I am the Senior Advisor and Director of Privacy
5 Policy in the Department of Homeland Security Privacy
6 Office and one of the coordinators of the workshop and
7 welcome you this morning. My role this morning is
8 very easy, I'm just going to do a couple of
9 housekeeping remarks. First of all, we appreciate
10 your patience in getting seated. I think we'll have
11 more people flowing in throughout the day. If you
12 have not already discovered the restroom facilities
13 are around the corner on this floor at the very end to
14 your left. They're all the way downstairs at the
15 bottom. In between you have to have a high tech key
16 card, which we don't have for you, so please use the
17 one on this floor or downstairs.

18 We've set aside 15 minutes for each panel,
19 towards the end of each panel for your participation,
20 your questions and contributions. So, you'll hear
21 from the moderator when it's time to line-up and there
22 is a microphone right here that you can use for that

1 purpose.

2 When we announced the workshop and fellow
3 register, we invited the public to provide comments on
4 a number of key questions regarding Government use of
5 social media. We will extend the comment period to
6 July 10th. So, if some of you, after hearing the
7 remarks during the workshop, have some comments that
8 you'd like to share with us, please do send them in.

9 I want to note that one of my colleagues from
10 TSA, Claire Barrett has made some "persistent cookie"
11 cookies. If you were one of the lucky ones who saw
12 them back on the water table, this is what you get
13 when you come to a Government program. You get the
14 employees themselves baking. We're unable to provide
15 you refreshments, but that's to keep our budget trim.
16 You'll have an opportunity at break time or at lunch.
17 There is a list of facilities for you at the front
18 desk if you haven't already picked up the sheet.

19 Please now silence your cell phones. Text
20 messaging, of course is permissible. This is a low
21 tech social mediate conference, but I think the
22 importance here is the face-to-face conversation that

1 we're going to have for the next day and a half. It's
2 my pleasure now to welcome my leader, Mary Ellen
3 Callahan, the Chief Privacy Officer of Department of
4 Homeland Security.

5 MS. CALLAHAN: Good morning and welcome. Thank
6 you all for coming today. It's a pleasure to see so
7 many colleagues from throughout the Government, as
8 well as, colleagues from outside the Government
9 including those who I have known in my past life.
10 With that said, I want to welcome you. As Chief
11 Privacy Officer, I want to welcome you to our workshop
12 Government 2.0 Privacy and Best Practices. Your
13 participation here and it is indeed a sellout crowd
14 today, is evidence that there is a great need for this
15 program. Agencies across the Government are grappling
16 with the same challenge, how do we engage in social
17 media while protecting individual privacy. At the
18 very beginning of his Administration President Obama
19 announced his goals of transparency, participation, and
20 collaboration. I strongly support the role Government
21 2.0 can play in achieving these very important goals.
22 We know that reaching these goals will require

1 creativity and innovation. It will also challenge our
2 ability to take our privacy laws and apply them to new
3 platforms. However, I'm confident we'll be able to do
4 that if we work together leveraging expertise inside
5 and outside the Government.

6 Attendees here today come from almost every
7 Federal agency, large and small and from many interest
8 groups working on issues related to social media and
9 privacy. Our panelists are leaders in their field, as
10 well and they have spent a great of time participating
11 and preparing for this workshop and I want to
12 personally thank them for doing so and for making this
13 to be a very useful exchange. I'm also delighted that
14 White House Chief Information Officer, Vivek Kundra
15 and Deputy Chief Technology Officer, Beth Noveck both
16 leaders in the Administration's efforts to
17 dramatically increase public involvement through
18 social media are both going to be able to share their
19 visions on how it will happen. Vivek today and Beth
20 tomorrow and I want to thank them both for joining us.

21 I hope you will attend all of the workshop panels
22 as each is designed to build one on top of the other.

1 With that said, I want to briefly describe the panels
2 so you can know what to look forward to.

3 The first panel will showcase how Government
4 agencies are currently using social media and
5 highlight some of the policy decisions agencies have
6 made along the way. We'll then break for lunch and
7 reconvene in our second panel, which will identify the
8 various ways in which the Government's use of social
9 media may impact individual privacy. The privacy
10 impact session will then be followed on a panel on
11 security issues posed by Government's use of social
12 media and as I mentioned, our workshop tomorrow will
13 continue with opening remarks by Beth Noveck, who
14 leads the Open Government Initiative. Our first panel
15 tomorrow will bring together experts who will explore
16 a broad range of the legal issues posed by Government
17 use of social media. And then we'll close with a
18 panel of experts who have given considerable thought
19 to identifying best practices that can support the
20 Government's use of social media in a way that's also
21 respectful to privacy and the privacy laws.

22 To be clear, privacy and active involvement with

1 Government through social media are not mutually
2 exclusive and the challenge we face, though is how to
3 engage the public and individuals and provide
4 individual control over the information they chose to
5 share with the Government. I expect this workshop
6 will go a long way towards meeting that challenge.

7 Once again, I want to thank the panelists,
8 speakers and all of you for your participation in the
9 workshop. I know we will all benefit from having
10 worked through these important policy issues that
11 confront us, decisions that need to be made now. I
12 regret that due to an international obligation, I
13 cannot attend the entire workshop, but my staff is
14 here and they will certainly assist you in any way and
15 will be preparing report at the conclusion of this
16 workshop that we hope will be useful for people both
17 inside and outside the Government.

18 It's now my distinct pleasure to introduce Vivek
19 Kundra. Vivek was appointed the first Federal Chief
20 Information Officer (CIO) of the United States by
21 President Obama in March, 2009. In that role, he
22 directs the policy and strategic planning of Federal

1 information technology investments and is responsible
2 for the oversight of Federal technology spending. The
3 Federal CIO establishes and oversees enterprise
4 architecture to ensure system interoperability and
5 information sharing and to ensure information security
6 and privacy across the Federal Government.

7 I have thoroughly enjoyed working with Vivek
8 within the Federal CIO Council where he has shown some
9 great leadership already on important initiatives and
10 I want to thank him for taking that role.

11 Vivek Kundra has been recognized among the top 25
12 CTOs in the country and as the 2008 IT Executive of the
13 Year for pioneering work to drive transparency, engage
14 citizens and lower the cost of Government operations.
15 Prior to joining the Obama Administration, Vivek
16 served in Mayor Fenty's cabinet, as a CTO for the D.C.
17 Government and Governor Kane's cabinet as Assistant
18 Secretary of Commerce and Technology for the
19 Commonwealth of Virginia. His leadership and vision
20 are blazing a trail for the Federal Government in a
21 wide range of technology issues and I look forward to
22 hearing about his vision for Government 2.0; Vivek.

1 MR. KUNDRA: Thanks Mary for that kind
2 introduction. Good morning everyone. How's everyone
3 doing? Privacy is one of the key topics that's very
4 near and dear to myself and especially when we talk
5 about privacy in the context of innovation and what
6 we're trying to do in the Obama Administration.

7 For far too long I believe that people have
8 thought about privacy as being in direct conflict to
9 innovation and driving agenda where we're leveraging
10 some of these new Web 2.0 technologies and it's
11 actually true with security also. For far too long
12 people have looked at security through the same lens.
13 One of challenges that we face in the Administration,
14 as we think about privacy, as we think about
15 information security and innovation overall is to look
16 at statutes that have existed, if you look at the 1974
17 Privacy Act. If you look at what's happening in terms
18 of the Cookies Policy, if you look at some of the
19 other statues that are in place, they've been in place
20 for a while and one of the challenges is that as
21 technology has evolved our Legislation and our
22 approach and the Federal Government's role in

1 embracing new technologies to make sure that it is
2 compliant, number one. And number two, to look at
3 innovations that have happened in the market place
4 hasn't kept up to pace with what's happening out
5 there.

6 So, what are we doing within the Federal CIO
7 Council? The first thing we did, actually is we've
8 moved forward and we've created a dedicated working
9 group that Mary is helping lead in terms of privacy
10 and making sure that as we move aggressively in
11 adopting some of these new technologies that we
12 actually bake privacy into the architecture of the
13 solutions rather than thinking about privacy as an
14 after thought and trying to bolt it on after we've
15 already deployed some of these solutions.

16 One of the most interesting conversations I
17 actually had coming into the White House, when we were
18 talking about public participation was not about how
19 do we go out there and create infrastructure that
20 secure ties everything in terms of people's
21 interaction with Government. It was actually about
22 how do we deploy the ability to provide anonymous

1 feedback to the Government. So, we sat there and
2 we talked about, well how do we make sure that as we
3 engage the American people we can do so in a manner
4 that they're comfortable, in a manner where their
5 privacy is protected and where they can provide us the
6 most honest feedback possible from a public
7 prospective as we make some decisions around
8 regulations as we talk about the Open Government
9 Directive. If you looked at the President's Town Hall
10 meeting, we spent a lot of time thinking about how
11 we'd make sure that the feedback was anonymous. That
12 people were able to provide us their feedback in a way
13 that protected their privacy.

14 At the same time, that makes up a small
15 percentage of a much larger equation when we think of
16 information technology investments. The Federal
17 Government today has over 10,000 systems and spends
18 over \$70 billion dollars annually on information
19 technology. What's vital is as we think about these
20 systems, some of them are old 30, 40 plus year old
21 systems that are built on foundations on technologies
22 like Cobalt, other systems that we continue to invest

1 in to keep them operating and also, third are systems
2 that we're actually buying.

3 Across the board there was a phenomenon in the
4 early '90s. Of course, what ended up happening was
5 the Government essentially took its business practices
6 in those systems and essentially Webified itself. It
7 did not make the tough changes that it needed to make
8 on the back end. In terms of looking at those
9 systems, looking at their workflows and re-
10 engineering. That's the hard work of transformation.
11 Now, as we move forward what we've noticed, of course
12 is in a context of upgrading the systems, in the
13 context of providing you services that we can't
14 continue to just webify those systems, we have to take
15 on those tough issues. We have to ask the questions
16 in terms of how are we making sure that we're
17 protecting privacy, especially when it comes to
18 security. It's easy to tilt in the direction where
19 you're monitoring everything. It's easy to tilt in the
20 direction where the default setting is as anybody
21 touches Government systems that we're going to try to
22 do whatever we can in terms of scanning, in terms of

1 monitoring activity rather than making the tough
2 decisions around how do we make sure as a principle
3 that the privacy and security of the American people
4 are protected. That's one of the areas that we're
5 very focused on, especially as we move into this Web
6 2.0 world.

7 One of the things that I've been talking about is
8 this notion of a context driven Government, which
9 opens up a whole host of privacy issues. That world
10 that we have to think about is a universe where we
11 look at some of these networks that exist today.
12 Facebook, for example has over 200 million users out
13 of which 56 million are in the United States. If you
14 look at what eBay does, every minute there is a car on
15 eBay, 10 billion transactions on a monthly basis, the
16 same thing with Craigslist.

17 Now, we've continued in the past to look at
18 Government and look at these systems and we've
19 essentially said, well we're going to webify what the
20 Government already has and the Government historically
21 has invested a fortune in building up infrastructures
22 and platforms that are actually available in the

1 commercial space and that are available at low cost.
2 So, how do we balance the ability to make sure that
3 our policies in the Federal Government and the
4 technologies that we're investing in allow us to make
5 sure that those issues are addressed, especially when
6 we think about Government services? Why isn't it that
7 we're providing services in the right context? So,
8 consider this for example. From birth to death, the
9 average person and how they interact with Government
10 is very different. You may not care about a birth
11 certificate at the age of five, but it maybe the most
12 important thing when you're born. You may not care
13 about a driver's license until you're in your teen
14 years or you may not care about mortgages and taxes
15 and business formation. Yet, for far to long what
16 we've done is we've created institutions where they're
17 mirrored in the digital world. We haven't taken
18 advantage of the Web 2.0 world. That's one of the
19 reasons we've ended up with over 24,000 Web sites
20 across the Federal Government. Imagine as an
21 individual, if you're trying to, as a constituent
22 access Government services, you have to navigate the

1 physical bureaucracy online because it was mirrored.
2 At the same time, consider the complexity that exists
3 from a services perspective. If you were to start-up
4 a business today, you've got to be able to interact
5 with your local Government, with your State Government
6 or the Federal Government and across the board.
7 You've got to fill out a number of forms. You've got
8 to wait for the processes. Yet, where technology is
9 headed and where the consumers are headed, the
10 constituents are demanding for the greatest ease in
11 providing services is to abstract all those layers.
12 People don't want to have to worry about, am I filing
13 local, State or Federal. The easiest thing to do
14 would be to abstract those layers to allow people to
15 have access to those services in a seamless way. Now,
16 that of course opens up a lot of issues around
17 information sharing as we extract the systems, as you
18 allow for a greater interoperability and all those
19 policies associated with information sharing. It
20 opens up a whole host of issues that are on security,
21 also. Those are some of the core policies we're
22 looking at. I recall, as we were looking at whether

1 it was a cookie policy for sharing videos or whether
2 we were looking at policies around the Presidential
3 Records Act or policies around the Paperwork Reduction
4 Act, we've got to figure out how do we ensure that as
5 we move in this direction that we protect the privacy
6 of the American people as I've said, but at the same
7 time look at technologies that can help us address
8 some of those issues. It's not a -- game because
9 there are a lot of innovations where people can
10 progressively decide in which terms they want to
11 interact with the Government rather than the
12 Government deciding unilaterally the terms under which
13 the American people will interact with them. To that
14 end, with the privacy counsel we're looking at the
15 impact especially when we move towards this context
16 driven Government model. What do we need to address?
17 What are the core issues around there? Especially,
18 when you start thinking about these issues and then
19 you're traveling internationally at an international
20 level. What happens at an international level? The
21 same fundamental issues that we face during our 60 day
22 review on cyber security and one of the reasons the

1 President had made sure that there was a Privacy
2 Officer at the National Security Council as we look at
3 some of these cyber issues and as the President is
4 committed to making sure that we will not; and as he
5 said, "We will not monitor private traffic on the
6 Internet as we move toward security." From an
7 international perspective, as we look at some of these
8 big issues around whether it's information sharing.
9 If you think about the H1N1 Flu, how do we make sure
10 that on one hand we're able to share information? On
11 the other hand, we're able to provide and protect the
12 privacy of the people. I would argue that there's a
13 lot of innovation that's happened in this space and
14 the answer actually lies in a couple of areas. One is
15 in technology itself. If you looked at some of the
16 algorithms that have been developed within the
17 financial services market or whether you look at
18 what's happening in the search space, they've been
19 able to -- data in a way that allows privacy to be
20 protected, but are able to provide you with higher
21 quality in terms of security.

22 The second space that we need to look at is

1 what's happening, as far as, public policy debate and
2 I think it's important to make sure that as we're
3 having a discussion on privacy that we don't divorce
4 it from security itself either because it can slice in
5 multiple ways in the same way in terms of looking at
6 security and privacy and what do we need to do to make
7 sure that they're both baked into the architecture,
8 the culture, the DNA of how the Government operates
9 and how we actually make those acquisitions.

10 Which leads me to the third point, which is how
11 we buy systems. For far too long I think we've been
12 buying systems across the Federal Government and
13 moving forward with transformations without really
14 engineering privacy and security into those systems.
15 One of the things we're doing is we're making sure as
16 we look at procurement transformation that that's also
17 part of the solution, making sure that we're
18 addressing those issues upfront rather than coming
19 back and saying, well, what do we need to do now that
20 we have invested millions or billions of dollars in
21 these systems to make sure that they're compliant.

22 So, with that I would love to take any questions

1 and I look forward to working with each of you as we
2 move forward in this new world. It very much reminds
3 me of a book that I read called, "Undaunted Courage",
4 but I learned -- as we move into this new world I
5 think there are great opportunities as we look at the
6 potential of Web 2.0, Government 2.0. At the same
7 time we need to be mindful that as we move into this
8 world aggressively that we don't do it at the cost of
9 privacy and security. Thank you very much. Mary, do
10 we have time for questions?

11 MS. CALLAHAN: Yes, we have time for questions.
12 If you have questions for Vivek please come to the
13 microphone.

14 AUDIENCE PARTICIPANT: Sir, are you considering
15 then modification to the Federal Acquisition
16 Regulation clauses for mandatory inclusion? Arguably
17 the current Privacy Clauses, Part 24 are incredibly
18 weak with regards to mandatory enforcement of the
19 Privacy Act. They don't relate particularly well to
20 the information systems. There are stronger FAR
21 clauses relating to information systems, but they're
22 not in FAR Part 24. Are you considering review in

1 mandatory enforcement?

2 MR. KUNDRA: So, we're considering review of the
3 entire procurement system. Obviously, we're looking
4 at it. But before we even jump into what we're going
5 to tweak on the procurement side. One of the
6 interesting challenges is not the how, but the what.
7 So, the first order question is as we're looking at
8 it, for the privacy committee what does it mean in a
9 Web 2.0 world in terms of how do we make sure that
10 we're protecting privacy and what are the policies
11 that need to be guided in that direction. That I
12 think is a larger issue. On the execution side,
13 absolutely we're looking at whether it's the -- we're
14 looking also at specific contracts in terms of how do
15 we bake that directly into contract when it comes to
16 privacy. I'm also recognizing that not all systems
17 are engineered the same way or serve the same
18 missions. So, certain systems are going to require
19 far greater oversight when it comes to privacy and
20 security. Moving toward a model where we're looking
21 at certain classes versus those systems that are not
22 really going to have sensitive data or sensitive

1 information.

2 AUDIENCE PARTICIPANT: Jeremy Duffy from the
3 Interagency Support Staff. It's great that I hear you
4 saying things about making privacy in the future in
5 the Government and that's a good thing. I'm curious
6 what's your position on taking care of the privacy
7 problems we have now, specifically State records
8 online, which create a huge privacy problem and
9 security problem for everyone because of identity
10 theft and what have you? I understand they're public
11 records, but there's a big difference between publicly
12 accessible and world accessible through the Internet
13 at all hours.

14 MR. KUNDRA: So, on that point what we're doing
15 right now and one of the reasons that the President
16 actually even commissioned the 60 day review, one of
17 the key findings there has been that the White House
18 must lead on this important issue because you've got
19 so many bodies across the Federal Government, entities
20 and institutions looking at these issues that we
21 haven't had historically, a coordinated approach,
22 number one.

1 Number two, what we need to be able to do as soon
2 as the coordinator is appointed is we need to be able
3 to look at where we are, not only current state, which
4 is important, but when we look at all the public
5 records issues that you're talking about the Paperwork
6 Reduction Act (PRA) those are all the issues on the
7 table and I'm working very closely with -- at OMB as
8 we move forward in terms of, one making sure that
9 agencies are complying with statutes and number two,
10 looking at where we're headed.

11 AUDIENCE PARTICIPANT: I'm wondering, regarding
12 the use of social media for emergency communications.
13 What types of policies do you suggest or do you see
14 coming in the future for the use of social media in an
15 emergency communications, but as a more collaborative
16 effort across agencies, the same sort of baking it
17 into these policies that we're now creating rather
18 than adding it on later when we realize that it's
19 another capability? And also what types of policies
20 need to be enacted for making it safer for information
21 against Homeland Security threats that kind of thing,
22 if you have a larger picture of information coming

1 out?

2 MR. KUNDRA: Sure. That gets into a model with
3 what we've done with data.gov where we've actually
4 launched a platform that allows for innovation to
5 happen and we've already noticed that people are
6 taking what we put out there in terms of a platform
7 and they're innovated. Now, from an agency
8 perspective if you look at what CDC has been doing
9 with H1N1 with the widgets that they've built, they
10 way they're disseminating information. They're fully
11 moving forward in terms of implementing some of the
12 social media aspects as far as communication is
13 concern. What we're in the process of doing is
14 because technology, by the way has evolved much faster
15 than the policies that I've been mentioned, we're
16 trying to make sure as we look at these policies that
17 they allow people, one to be able to leverage the
18 social media tools and two, also at the same time are
19 compliant with statutes. Not to say that some to the
20 statutes when they were originally written frankly in
21 an era that was very paper based, how do you make sure
22 that now in a digital media era that you're able to

1 re-look at some of those statutes and figure out what
2 makes sense and what doesn't make sense as we move
3 forward where the prime principle, the prime directive
4 being that we need to make sure that we protect
5 privacy?

6 AUDIENCE PARTICIPANT: Hi, Brenda Abrams from
7 Department of Treasury Office of Cyber Security. You
8 talked earlier about business process re-engineering
9 and how we need to bite the bullet and move forward in
10 order to enable these new technologies, especially
11 social media to be able to be implemented in this
12 secure environment. So, my question to you is, what
13 are you going to do to move Government off of that
14 dime and move them forward and do the hard work?
15 Because many people have tried this approach, to get
16 the hard work done and I have both seen that from the
17 Government perspective, as also a former consultant
18 and I really would like to hear your plan for getting
19 that moved forward. Because we need all the new
20 technologies in order to make Government to move
21 faster, more efficient and definitely in a more secure
22 way.

1 MR. KUNDRA: Sure. One of the things we're
2 actually doing is at the end of June we're going to be
3 launching a dashboard, IT dashboard. That's going to
4 give you transparency and visibility into the \$70
5 plus billion dollars of IT expenditures. So, you'll
6 actually be able to see for the first time across the
7 Federal Government every single major IT investment,
8 where it stands, what's the impact, what are the
9 dividends, who is the CIO in charge and not only that,
10 but you'll be able to see where they stand on a real
11 time basis in terms of schedule and cost and the
12 companies that are involved in doing that work. I
13 believe that's first order in terms of making sure
14 that we're transparent about how we're spending our IT
15 dollars today.

16 Second is being able to make the tough choices in
17 terms of being able to divest from programs that are
18 not producing the dividends that they were expected to
19 produce and invest in programs that are actually
20 producing the dividends that we're looking for.

21 The other areas, I think the White House is
22 leading. If you look at what the White House is doing

1 in terms of whitehouse.gov and some of the tools that
2 we're leveraging in terms of setting the tone for
3 public participation, backing transformation,
4 leveraging platforms that are low cost at the same
5 time provide you the meaningful transformation that
6 we're looking for because not every solution in the
7 public sector has to cost hundreds of millions of
8 dollars. There are many light weight solutions that
9 are available. One of the examples I used is where
10 you have one agency that was going to spend about
11 \$600,000.00 on a blog and there're three platforms out
12 there that could provide the same solution and wiser
13 minds prevailed and they leveraged the first solution.
14 So, a couple of things. One, be extremely transparent
15 about how you're making those investments. Two, lead
16 from the White House in terms of leveraging some of
17 those tools. And number three, drive that change
18 through the CIO Council.

19 AUDIENCE PARTICIPANT: Peter Swire, Ohio State
20 University and Center for American Progress. I have a
21 question on the legal side. I'm on the legal panel
22 tomorrow and agency lawyers, as you look at all the

1 2.0 sorts of things, some of them are struggling to
2 see how to make things fit within the current laws.
3 So, my question to you is as you do these reviews is
4 there an openness to possibly go into Congress in
5 seeking statutory changes if you find areas where the
6 paper based statutes don't fit so well for today? Do
7 you have anything to say about possibly being open to
8 going to the Hill if need be?

9 MR. KUNDRA: So, I think again as I mentioned
10 before around security and privacy, one of the things
11 we're already doing is there are a number of pieces of
12 legislation when it comes to actually even privacy
13 baked in with some of the security bills. So, what
14 we're doing right now is we're looking at all the
15 legislation because one of the things we have to make
16 sure is that it's harmonized across the Federal
17 Government. So, with the new Cyber Coordinator I will
18 be working to make sure that the changes that are
19 necessary can be made and to lead us to a place where
20 we can leverage some of these technologies.

21 AUDIENCE PARTICIPANT: Robert Ferrin, USCIS. I'm
22 interested in your comment that you said that we're

1 going to leverage the technology itself to protect
2 privacy and I've been looking at issues related to
3 identity management. So, in the context of citizen
4 access to their own information, how can you project
5 the way of both allowing access and perhaps
6 solidifying identity to assure the assurance of
7 security and privacy in that prospect?

8 MR. KUNDRA: I think if you look at identity
9 management, the default position has been that
10 everything has to be 100% secure. Everything is sort
11 of looked at from a military grade perspective.
12 What that has done has made the adoption of some of
13 these new technologies extremely difficult rather than
14 saying, well how do we move towards an environment
15 where we've got progressive credentialing? What I
16 mean by that is as a United States citizen there may be
17 a point where I want to interact with the Government
18 on an anonymous basis because I want to get public
19 input. There maybe another point where I only want
20 the Government to know my name and maybe my social
21 number versus another transaction that maybe much more
22 restrictive in nature sensitive where you have to

1 share more information. So, rather than treating all
2 classes of transactions as the same, we need to move
3 to an era where we're able to look at risks and we're
4 able to look at sensitivity and privacy of
5 information. So, where does it make sense to have
6 anonymous identity versus identity with user ID
7 password versus where you've got a smart card so you
8 know exactly who that person is and you're looking at
9 multifactor authentication? So, the key is how do you
10 make sure that as you deploy these systems that you're
11 able to look at and model it when it comes to identity
12 management, which is progressive in nature and not the
13 lowest common denominator for every single transaction
14 possible because agencies have different missions and
15 there are various transactions. Especially, it gets
16 interesting when you start looking at State and local
17 Government coupled with Federal Government. So, thank
18 you so much.

19 MODERATOR SAND: Thank you very much. I want to
20 invite the panelists for Panel One to come to the stage
21 and take your seats here. Also, this is a social
22 networking workshop and we have people who are

1 standing. If there are empty seats next to you or
2 your bags are on the seat, please extend that social
3 invitation and create some space for them. I'm also
4 going to ask the panelists to understand if somebody
5 takes your seat while you're sitting up here because
6 we're going to be up here for a little bit. So,
7 people in the back if you see an empty seat, please
8 sit in it.

9 MS. CALLAHAN: I don't know if anybody else is
10 Twittering the event. I also don't know if anybody
11 has created a house tag. I'm using "DHSPRIVACY".

12 MODERATOR SAND: This is the first working panel
13 of the workshop. The goal here is to lay the
14 foundation for the rest of the workshop and to give
15 you an understanding of the technology for those who
16 are new to it, but certainly for everybody to give you
17 a sense of what this stuff looks like and to actually
18 hear from the people who are creating it, what their
19 vision is in creating it and how they want to use it
20 and what it was like to actually build that and then
21 also to give you an opportunity to ask questions
22 directly to the people who actually built these

1 experiences for you.

2 We have two sessions in this first panel. In
3 the first session we're going to have three speakers
4 and then 15 minutes for you to ask questions of us and
5 then we're going to have a break, about 15 minutes and
6 then come back for the second sessions. Again, three
7 speakers, a 15 minute opportunity to ask questions and
8 then we'll go to lunch. I encourage you to ask as
9 many questions as you can to the people here because
10 these are the people who have actually created it and
11 might give you a very interactive opportunity to talk
12 to the people who are delivering these services.

13 I'm going to ask the panelists just quickly to go
14 through, give the audience who you are, where you're
15 from and just a quick one liner of what you plan to
16 talk about then I'll sit down and we'll go into the
17 presentation.

18 MS. TELLER: Good morning, I'm Maxine Teller. I
19 have a company called MiXT Media Strategies. I do
20 social media and collaboration business strategy
21 consulting. One of the clients that I work with is
22 the Department of Defense Public Affairs Emerging

1 Media Directorate. I've been working with them for a
2 couple of years so I'm here with two hats on today.
3 First, part of my presentation will talk about more
4 general big trends, what social media is all about and
5 why is it important. Then the second half I'll talk
6 about my Department of Defense case study.

7 MR. RICHE: Good morning everyone, I'm Victor
8 Riche and I head the Technology Office which supports
9 the public diplomacy mission of the Department of
10 State. I grew up in New York City and I learned
11 everything playing stickball at PS-45 and I look
12 forward to playing and sharing with you today what
13 we're doing with social media at the Department.

14 MS. CRAMER: Hi, I'm Jodie Cramer. I'm an
15 attorney at the Federal Emergency Management Agency
16 (FEMA) and I am Legal Counsel to our social media
17 program. I'm going to talk about what we've done and
18 how we started in 2007 with our social media program
19 and some of the policy groups that we've created.

20 MS. TRUDEAU: I'm Lena Trudeau. I'm with the
21 National Academy of Public Administration. The
22 National Academy is a non-profit non-partisan

1 organization that is chartered by Congress. As part
2 of the work that we do in Government, part of our
3 charter asks us to look across Government and better
4 understand and how Government agencies better
5 understand how trends are changing the face of public
6 administration. One of those trends we've been
7 looking at for a couple of years now is that of Web
8 2.0. I'm going to speak a little bit about what we're
9 doing at the National Academy in this space, but also
10 what we're seeing across Government.

11 MR. BURNS: Good morning, my name is Bob Burns
12 otherwise known as "Blogger Bob" from the TSA Blog
13 Team. I'm here today on behalf of Lynn Dean as you
14 can tell on my fancy name tag here. She's currently
15 going cross country in an RV, across the United
16 States, so she couldn't be here today. I'll be
17 talking about best practices on the TSA blog, things
18 we've done to be successful. Otherwise, we're using
19 social media internally and externally.

20 MR. AMES: Good morning I am Jeremy Ames. I
21 work for the Indoor Environments Program with EPA,
22 which is a small program within a big regulatory

1 agency. I'm going to talk about how we stumbled into
2 social media. Stumbled is probably accurate,
3 primarily for public outreach and increasingly
4 stakeholder engagement and collaboration.

5 MODERATOR SAND: Just one final note for the
6 panelists. You can stay where you are and flip the
7 slides this way or come to the podium and do it, your
8 pleasure.

9 MS. TELLER: I'm going to start by telling you a
10 little secret. Social media is not about tools and
11 technologies. It's really not. It's about human
12 interaction and communication and if it's really about
13 human interaction and communication why is this stuff
14 so intimidating and so overwhelming and so foreign to
15 so many of us. Well, I'm going to give a little walk
16 back in history for just a couple of minutes to
17 explain why. So, in the nineteenth century; yes this
18 is the Ingalls Family from Little House on the
19 Prairie. The nineteenth century was really all about
20 participation. People helped one another in their
21 communities. They lived a pretty transparent
22 existence, everybody kind of knew everybody's business

1 and they collaborated. If somebody needed a barn
2 built, the community came together to help them build
3 that barn. So, yes in the first two seconds here I've
4 used the three most popular words of social media buzz
5 right now and of the Obama Administration in
6 messaging; participation, transparency and
7 collaboration.

8 So, then came the Broadcaster Act and advances in
9 technology and made travel more accessible and
10 affordable and people distributed and they moved and
11 broadcast was invented and it enabled us to sort of
12 connect the country and the world and overcome the
13 challenges of distribution and of distance. Big media
14 organizations reigned and the power of broadcast
15 media's reach was unprecedented in the 20th Century.
16 Radio, TV and newspapers solved the challenges of time
17 and place and brought people together. News reached
18 far and wide. But at the same time, in a lot of ways
19 broadcast distanced us from our communities because it
20 was one way, it wasn't interactive and it wasn't
21 participatory. It kind of removed that human
22 interaction component. So, here we are in the 21st

1 Century and I refer the 21st Century as the
2 collaboration era. I know this beautiful peacock
3 looking thing is actually not the NBC peacock from the
4 broadcast era. It's a piece that was done by Brian
5 Solis and Jessie Thomas of Just Three, called "The
6 Conversation," and it shows social media tools and
7 technologies. There are faster, cheaper bandwidths
8 today has enabled the invention of a whole new set of
9 tools and technologies and they provide us with two-
10 way interaction. It's a very different take than the
11 broadcast era. Social networks, blogs other social
12 media platforms afford individuals and organizations
13 access to the same information and capabilities that
14 were previously only available to big media
15 organizations. To level the playing field social
16 media tools enable us to do things differently. In
17 fact they encourage us to do things differently and
18 they push the boundaries and challenge our assumptions
19 and what we grew up with and they're a big deal.
20 They're not a big deal because they're hip and trendy
21 right now and they're not a big deal because they have
22 cute names like Twitter and FriendFeed and they're not

1 even a big deal because over half of Americans are
2 using them each and every day. They're a big deal
3 because they're changing the ways that we interact and
4 communicate with one another.

5 Individuals, businesses and media organizations
6 really have the same access to information and you to
7 can have influenced the rivals, the most widely
8 syndicated columnist or the most well remembered Super
9 Bowl ad, the price, transparency, participation and
10 collaboration. But here's the disconnect we're
11 products of the broadcast era. We don't know how to
12 do this, we're used to one way communication, we're
13 used to receiving messages and now we're in this world
14 where collaboration is the name of the game. We kind
15 of don't know how to do that. We're not so familiar
16 with the two-way. In some ways if you'd presented our
17 nineteenth century ancestors with this it would've
18 been more familiar to them, the actual interaction.
19 But social media is catalyzing a cultural shift.
20 People can in fact use information just as
21 organizations can. It enables us not to just talk and
22 interact with news organizations, but also with one

1 another. Our current customers, employees and
2 citizens are tasting and trialing all of this new
3 technology and they're wowed. It's changing their
4 expectations. They're seeing that there are better
5 ways to share photos, there are better ways to invite
6 people to events, there are better ways to discuss
7 news of the day. They're no longer waiting for the
8 broadcast, they're participating, they're engaged, and
9 they're leading the conversation.

10 Our future customers, employees, and citizens
11 don't think like we do. They are digital natives.
12 That means they were born in or more recently than
13 1982 and they've only known the world that's digital,
14 where everything is available at the touch of a
15 button. Every news bite, every sports score
16 everything that they want, as long as, they have
17 access to the Internet on a mobile device, on a PC
18 they can get anything that they want any time. It's a
19 very different orientation. As you can see 93% use
20 the Internet, 97% game, 75% are on social networks,
21 75% tax there and this. People use this regularly.
22 The rest of us are starting to have content

1 expectations more like digital natives. Collaboration
2 is not just their expectation, it's their instinct.
3 This is how the next generation thinks. But here's
4 the challenge. It's a bit of "catch 22" for the rest
5 of us. Wanting to collaborate, unless you understood
6 the importance and the value of collaboration and you
7 can't possibly understand the value of it until you
8 start doing it, so it's a "catch 22." The same is
9 true of social media. You're not going to use these
10 tools and technologies until you understand the value
11 of using them and yet you can't possibly understand
12 the extent of the value until you start using them.
13 It becomes more complicated in this way. These two
14 "catch 22s" affect one another. So, I don't know it's
15 a "catch 44", a new term. If you understand the value
16 of collaboration you see that these tools and
17 technologies enable that and help that. If you
18 understand that you'll use them more and you'll
19 collaborate more and it goes on and on through the
20 infinite sign that you see.

21 The challenges, it kind of requires a leap of
22 faith to start in on this or in our case a

1 Presidential memorandum. So, I'm going to stop with
2 all of this. Wait until the end for questions.

3 MODERATOR SAND: You don't have enough time.

4 MS. TELLER: Okay, so I'm not going to let you
5 ask questions. I'm going to talk a little bit about
6 the work we've done at Department of Defense and how
7 all of this plays out. I'll start with a video.

8 (Video Playing)

9 MS. TELLER: So, the group that I work with at
10 the Department of Defense is the Emerging Media
11 Directorate. It sits within the Defense Media
12 Activity, which is kind of a coming together of all
13 the media activities across the services and across
14 the Department of Defense. It was stood up in October
15 2008 as part of BRAC (Base Realignment and Closure)
16 and it really brings together all of the ways that the
17 Department of Defense communicates with citizens and
18 as I said it sits within Public Affairs.

19 So, we've been very lucky, the Department of
20 Defense because emerging media and new media is kind
21 of baked in as Vivek Kundra talked about. It's baked
22 into the 2006 QDR (Quadrennial Defense Review). So,

1 we really have had support from the top of the
2 organization since our beginning. As Secretary Gates
3 said in the video, we need new systems for the 21st
4 century. He said it better than I could. At the same
5 time, we also have tremendous bottom up influence
6 that's forcing us to do this, embrace social media
7 tools and technologies. There are 2.6 million members
8 of the U.S. Arm Forces and over 60% of them are digital
9 natives. This is how they communicate. So, if we
10 want to reach or audience, we have to do this, it's
11 not a question.

12 The Emerging Media Directorate started as part of
13 internal communications trying to reach the internal
14 audience, service members, veterans, Department of
15 Defense civilians, etc. But of course as soon as you
16 put something out on the Web it's available to
17 everybody. So, our audience is really the American
18 public.

19 The other thing that new media influences
20 is traditional media. 70% of journalists follow more
21 than one blog or at least one blog. 44% use social
22 networking sites for their reporting. So, one of the

1 things that we're interested in is the crossover. If
2 we put things out through social media, we often time
3 see these things, these words, these phrases popup
4 later in mainstream media. And I'll get into detail
5 on some of that in a minute. New media fills the gap
6 between public interest and media coverage. So, in
7 2008 the Pew Center for Excellence in Journalism did a
8 study looking at over 70,000 new stories from 2007 and
9 they looked at Americans' interest in particular
10 topics compared to the actual news coverage in
11 traditional media and they found a tremendous
12 disconnect in a lot categories. People wanted to know
13 about this. They were extremely interested and it
14 wasn't being covered in traditional news. So, we took
15 particular notice to things such as troop surge
16 proposal, events in Iraq and Iraq home front.
17 Obviously, these are issues very important to the
18 Department of Defense and the Emerging Media
19 Directorate tries to help fill this gap and provide the
20 public with what they want to know, whether or not it's
21 being covered by mainstream media. The example that
22 we like to use is back in 2007; the U.S. won the Battle

1 on Haifa Street in Baghdad and it was a big deal. It
2 paved the way for the surge and we were getting
3 terrific coverage from the news media and then all of
4 a sudden after a couple of days it completely fell out
5 of the news cycle and no one was covering it anymore
6 and Public Affairs was, "What happened?" Well, what
7 happened in January 2007, big news event, the death of
8 Anna Nicole Smith and it was a little bit more
9 exciting for the news media to cover. This really
10 just cemented for us that we need to be telling our
11 own story, we need to take responsibility for the
12 messages that we know are important and that clearly
13 the American public is interested in. So, we tried to
14 figure out how to do that. We thought about bloggers
15 and that there are military bloggers that are out
16 there writing about this regardless of what's
17 happening in the news media. This is their beat. We
18 talked about how do we embed bloggers with troops in
19 Iraq and that was really pretty complicated. So, we
20 decided to use old technology to enable new
21 technology. We created something called, The Bloggers
22 Roundtable Program. What we do is use old

1 communications to enable new communications. We set up
2 a conference bridge and enabled military bloggers to
3 call in and ask questions of a Department of Defense
4 expert that we provide on a given topic that we
5 provide. And they call in anywhere from one to 30 more
6 bloggers and it's kind of like an audio press
7 conference for non-credentialed journalists and they ask
8 questions, they go back and they blog about it and
9 they write about whatever they want. We don't control
10 the message. The message can't be controlled. So,
11 it's Webcasted live on Blog Talk Radio. It is archived
12 as a podcast. It's transcribed by Federal News
13 Service. American Forces Press Service usually often
14 write stories about this as an event that was
15 happening and if you subscribe to our RSS Feed or our
16 email you can receive updates that way. So, we're
17 really using a lot of different media to get this
18 information out.

19 To date we've conducted over 400 interviews with
20 the Department of Defense officials through Bloggers
21 Roundtable Program. We have engaged 620 unique
22 bloggers since 2008 and have won a number of PR awards

1 and things like that, including the Public Relations Society of
2 America on this program. Another program that we have
3 is called DODvClips and there are two pieces to this.
4 One is we have our own YouTube like site called
5 dodvclips.mil. So, it's on a .mil regardless of
6 wherever you are, behind whatever firewall you can
7 access this. And that's why we did that. We put out
8 clips of video often times produced by the Pentagon
9 Channel. We also produce our own vlog, which is a
10 much more casual kind of fun way of communicating
11 video and bloggers can embed these pieces of video in
12 their sites, digital natives can watch these because
13 they're quick and we also have a channel on YouTube
14 with pretty much the same information on the DODvClip
15 site.

16 I guess really quick, let me just run through
17 principles of engagement. I just want to share with
18 you some of the important things to remember in
19 implementing programs, social media and new media
20 programs. Being mission driven is not about the tools
21 and technologies. It's about what you're trying to
22 accomplish and that hasn't changed and it isn't going

1 to change. It's just these are different ways of
2 communicating those messages and that information and
3 the roles are different. Just because you can doesn't
4 mean you should. A lot of folks come to me and say,
5 "We need a Twitter handle, give us a Facebook page."
6 And I say, "Why?" It's not about the fact that you
7 can. You have to have a very clear mission driven
8 reason why.

9 One of the things we did with Bloggers Roundtable
10 was to stop, look and listen. Before we started the
11 Bloggers Roundtable Program one of my colleagues who
12 is really terrific; many of you know Jack Holt, he
13 embedded himself in the blogosphere and the military
14 blogosphere and got a sense for who is out there, what
15 are they saying and he started to develop
16 relationships with them by responding in comments on
17 their blogs. Answering questions and setting the
18 record straight in ways that only the Department of
19 Defense can in this space and really taking tried and
20 true public affairs methodologies and applying them to
21 new media. It's important to listen to what's going
22 on before engaging to gain respective bloggers. It

1 doesn't work the same way as old media. Identify
2 where you should engage. Focus on where you, as a
3 Government agency can add unique value. Your
4 engagement is not going to be the same as the average
5 Joe. You're a Government agency. Stay in your lane.
6 Following public affairs guidelines is what we do
7 everyday at the Department of Defense and if you can
8 talk about it, you can talk about it and if you can't
9 talk about it, don't talk about it. I guess let
10 policy guide you, but not paralyze you. Operational
11 security rules still apply, seek to understand and
12 respect policies. Don't say, I'm a complete renegade.
13 I'm going to go against all policies. They're there
14 for a reason and they're really important. It doesn't
15 mean that they don't need to be tweaked. In some
16 cases they do, but seek first to understand. And then
17 reach out and participate. It's not about shoving
18 messages out there, but about engaging in the
19 conversation. It used to be that information was
20 power and I don't think that that's true anymore. I
21 think it's that information sharing multiplies power.
22 The more you put out there more you'll get back.

1 Big trust, and that's two parts, internally and
2 externally. I'm always happy to see workshops like
3 this because they're really cross functional and
4 they're bringing together people and organizations and
5 agencies who don't normally work together, but who
6 have to for this kind of thing. So, people support
7 what they help to create. The more you engage your
8 colleagues from other functions across your agencies,
9 the more support you're going to get from them.

10 And then externally, share that which is most
11 valuable and that's pretty -- usually you want to keep
12 behind a safe what's most valuable. But if you show
13 what's most valuable you get real feedback. You
14 develop trusted relationships and you'll get more
15 information back. You'll get more out of it than you
16 put into it.

17 We had a situation many months ago, it was
18 horrible a situation where a marine threw a puppy off
19 a cliff. Obviously, not a good thing for public
20 affairs to have to figure out. We looked at this and
21 said, "Oh, my God what are we going to do?" And we
22 decided to step back and just wait. The blogosphere

1 is very much a self correcting medium and we had built
2 relationships and trust out there and immediately
3 within an hour we knew who this guy was. There was a
4 Wikipedia entry, the video was posted on YouTube. We
5 knew what town he grew up in, what college he went to,
6 who his friends were, etc. Truthfully, the guy was
7 ruined. And that wasn't done by the Department of
8 Defense Public Affairs to protect this in some way or
9 get the story straight, it was actually the
10 blogosphere took care of it.

11 The last thing is commit to collaboration.
12 Collaboration is indeed everything. It's about
13 committing to an ongoing relationship. It's not a one
14 shot deal and about constantly innovating and thinking
15 of new and different ways to interact and add value to
16 the audience. Thanks.

17 MR. RICHE: Good morning, everybody again. I'd
18 like to thank Pete for inviting me today and also Pete
19 and Mike for going ahead and helping with the
20 technical things this morning. As I said I work at
21 the Department of State and I support the public
22 diplomacy mission of the Department. The mission of

1 public diplomacy is to inform, influence and a word
2 that you've already heard, engage foreign publics
3 overseas. So, we've been doing this for decades and
4 we've been doing it through exchange programs where we
5 bring people to the United States where they learn
6 about U.S. society and values. We've done it through
7 publications where we actually printed books. We
8 actually had something called libraries. Remember
9 when people went to the library and took out books?
10 We had libraries overseas. So, we've been doing,
11 informing, influencing and engaging for decades and
12 the Web has provided a whole new reader for us to
13 ahead and to do all of those things. We created a
14 Web site. This is our premier Web site. It's
15 America.gov. It's in several different languages and
16 it has a pretty large viewership. The audience though
17 is overseas. It's not supposed to be seen by people
18 domestically, but in the world of the Web it's
19 absolutely impossible to go ahead and to block that.
20 So, there is a law in the books that says we're not
21 supposed to show it or talk about it, but here it is.
22 I consider this to be a closed conference.

1 We've also moved very swiftly into the area of
2 social media because social media provides a perfect
3 digital compliment to everything that we've been doing
4 for decades. Not only have we done Web chats and Webcasts,
5 we've also used Twitter. We've done digital
6 video conferences, which is two-way in collaboration.
7 We created a mobile game that's used by about, I think
8 six or seven thousand people have already started
9 using it in the Middle East. We've also taken four
10 forays into Second Life. So, we're out there. We're
11 really trying to go ahead and inform, influence, and
12 engage the world and I'd like to go ahead and to show
13 you something that we did that's a little bit
14 different, at least for the Department of State.

15 (Video Playing)

16 MR. RICHE: Okay, this is not your typical
17 Department of State event. What we're trying to do is
18 to get people to go ahead and to submit videos that
19 they made that lasted up to three minutes to answer
20 the question, "Democracy is?" through video. The
21 contest was announced at the U.N. last September and
22 we received submissions from 95 countries worldwide

1 and the contestants who participated we announced the
2 winners just last week and I would say it was a
3 resounding success because it's generated a lot of
4 buzz in the field. People are talking about this,
5 they're sharing information and they're going to our
6 blog site from America.gov. They're talking about it
7 on our Facebook site on America.gov. So, it's done
8 what we've want it to do. We're thinking about going
9 ahead and doing another one bigger and better.

10 Another thing is that we've developed
11 partnerships with the private sector and also
12 universities, which also go ahead and amplify getting
13 our message worldwide. You can see the Motion Picture
14 Association, the Director's Guild and other
15 organizations that are very interested in video coming
16 in from around the globe. So, it just helps to build
17 the relationships that are absolutely tied perfectly
18 with social media. And I'd also like to go ahead and
19 show you one of the videos; but Pete has to help me
20 here; that was submitted for the contest.

21 (Video Playing)

22 MR. RICHE: Thank you, Pete. That came in from

1 overseas actually. That was not one of the winners,
2 but it's a short clip and it shows you the type of
3 product that we actually receive. Very innovative and
4 we have people around the globe answering the
5 question, "Democracy Is?" I would say that's really
6 expanding the role of public diplomacy in a really
7 neat way.

8 Okay, so what else have we been doing? Well, the
9 President gave a major speech in Cairo. That was the
10 first time a president ever went to Cairo and gave a
11 speech at the University of Cairo. He did it on June
12 4th and the name of the speech was "New Beginnings".
13 If you haven't seen it or heard it, you should go
14 ahead and find a copy of it and take a look at it.
15 It's really an excellent speech, but that's just me
16 Victor, not in my official role at the Department of
17 State. We really got geared up for this speech. It
18 was translated into 14 different languages that people
19 could go ahead and access from America.gov. People
20 were Twittering about the event. On that day it had
21 the second highest number of tweets that were on
22 Twitter because we created a hash tag to do that.

1 There's video that's been created and reused and it
2 was really a monumental effort. Now, one of the
3 things that we did that was a little bit different;
4 actually it was very different, we went ahead and we
5 allowed people to go ahead and sign up and receive
6 text excerpts from the President's speech and we went
7 ahead and had people translate the excerpts into
8 Farsi, Arabic and Urdu, which reaches a lot of the
9 Middle East all the way over into Pakistan. We
10 allowed people to go ahead and sign up where they
11 could go ahead and receive ten excerpts of the
12 President's speech and we only had three days to do
13 this. There were a few on my staff who didn't sleep
14 for those three days to go ahead and to get this set up
15 and we had about 5,000 people sign up. This type of
16 reach, because there are 4 million telephones out
17 there, we definitely want to grow this area. For his
18 next major speech, which is going to be in Ghana,
19 which is going to be July 10th and 11th, I'm sure that
20 we will double, triple and hopefully quadruple the
21 number of people receiving text messages for that
22 speech. So, that was really kind of cool.

1 The last thing that I would like to show you what
2 we're doing at the Department, this is in the area of
3 educational and cultural affairs. This is the program
4 where we bring up to 30,000 people to the United
5 States under various programs and sometimes they stay
6 here for a few weeks, sometimes they stay for a year
7 on the scholarship program, like the -- Scholarship
8 Program. These are some of the past participants that
9 are more notables, Tony Blair, the former Prime
10 Minister, Hamid Karzai who is the current President of
11 Afghanistan, Gerhard Schroder who was the head of
12 Germany and also Sarkozy the President of France was
13 also one of the people that were one of the past
14 participants on our programs. When we created a
15 social network, we launched it last October and this
16 little network here really created a ruckus in the
17 Department of State because it ends in .gov and we're
18 using a commercial provider as the framework for
19 handling all of the information that comes in from the
20 people who have joined this social network. The
21 reason we did that is not only because we have
22 flexibility, but a company called Ning did this for us

1 for a mere \$35.00 a month. So, I would say that that
2 was pretty good than going ahead and developing our
3 own. That's saving the taxpayers dollars. When we
4 did this we asked for their name, a valid email
5 address and date of birth. Definitely privacy
6 information, definitely all the alarms went off. We
7 had a huge meeting with people from the Privacy
8 Office, records management, the attorneys, the people
9 from IRM, diplomatic security. It was an unbelievable
10 meeting. I was there in the spotlight. I lost, I
11 think about four or five pounds just in that 45
12 minutes worth of meetings with the high level folks.
13 But the Under Secretary for Public Diplomacy and
14 Public Affairs at that time he said, "Surely, we can
15 work something out." Now, he's saying this to the top
16 legal advisor in the Department. He's saying it to
17 two Assistant Secretaries. He's saying it to high
18 level officials who deal with privacy day in and day
19 out and records management. Surely we can work
20 something out because this is the way that we're going
21 to be doing business from now on. So, what did we do?
22 I also head the Department's Internet Steering

1 Committee. So, I volunteered to go ahead and to start
2 a group to develop internal policies for the
3 Department because I knew that the Department did not
4 have one place where you could go ahead and find out
5 about social media and this is a copy of our wonderful
6 foreign affairs manual. But this is sort of the bible
7 for the Department of State. I'm working with some
8 key people to go ahead and to develop policies that
9 will address everybody's issues and we've been working
10 on them for several months. I'd like to point out my
11 colleague who knows all the details, who knows all of
12 the answers and if you ask me questions I'm going to
13 direct you to her, Sandy Simms. Sandy, stand up
14 please. She's a wonderful person. She knows all
15 about the policy. We've been meeting with the privacy
16 people, the records management, the attorney, you know
17 name it we've been meeting with all of them for
18 several months. I hope that we get the policy out.
19 Sometime in July it goes through a clearance and then
20 I also hope that it will be adopted and used in the
21 Department officially sometime towards the end of the
22 summer or beginning of autumn. This is a big deal.

1 It will be an official policy, guiding social media in
2 the Department and will also have guidelines attached
3 to it.

4 So, what's next? More of the same and bigger and
5 better. We have a new Under Secretary for Public
6 Diplomacy and Public Affairs and her name is Judith
7 McHale. She was the former CIO of the Discovery
8 Channel. She knows how to go ahead and to communicate
9 worldwide and she has said that we need to move
10 further into this area of social media and new media.
11 Up until a week and half ago I had five people working
12 in my office that did a lot of things in this area and
13 now they've been plucked out and moved into a new
14 media unit that's going to go ahead and report
15 directly to the Assistant Secretary for International
16 Information Programs, which is responsible for
17 America.gov. So, the Department is moving in a big
18 way in this area and it's just a perfect compliment
19 for public diplomacy. I thank everybody for listening
20 to me today and I look forward to talking to you later
21 on at the breaks and whenever. Have a great day,
22 thank you.

1 MS. CRAMER: Hi everybody, I'm Jodie Cramer. I'm
2 an attorney so I don't have any fancy video because
3 PowerPoint is hard for us. I work at the Federal
4 Emergency Management Agency (FEMA). We started in
5 2007. By 2007 we had a few rough years. I don't know
6 if you heard about our problems, but we were not the
7 media's favorite Federal agency or the public's.
8 There was actually a survey of the least favorite
9 Federal agencies and we ranked #1. It's kind of sad
10 for us because we give out billions of dollars of
11 money to individuals and to State and local
12 Governments. We ranked in front of the IRS and in
13 front of everyone else, the people who take money and
14 we give it away. So, it was very hard for us. So, in
15 2007 after there was a press conference problem; I
16 don't know if you heard about that one, we decided,
17 our Public Affairs Office decided they wanted to form
18 a YouTube channel, but luckily the person who was
19 assigned to setup the YouTube channel looked at the
20 terms of service and said, "I can't sign that." And
21 actually that was very wise of him and it ended up on
22 my desk as Legal Counsel. We started looking at the

1 issues associated with YouTube and what we noticed was
2 that we had a lot of issues with Web 2.0. There are
3 branding issues, there are legal issues, there are
4 record retention issues, there are staff and management
5 issues, there's IT security, there's privacy, and
6 there's a lot of coordination. Luckily, we're a
7 really small agency. We have about 3,500 permanent
8 employees. So, that's pretty small and a lot of us
9 are on the same two or three floors. So, we can
10 literally yell down the hall at each other. So, we're
11 pretty close and we can start yelling and saying, "Who
12 knows about this?" What we decided to do was we
13 looked at intra-agency cooperation and coordination.
14 The legal privacy people are coming together as are
15 our records management privacy with public affairs and
16 with IT and IT security and we came together and we
17 addressed all of these issues. What we ended up doing
18 is in 2008 we launched our YouTube channel, which was
19 the first agreement with YouTube by a Federal agency.
20 Hopefully this works and when I click on it you can
21 see our YouTube channel. We have our lovely policy
22 down here telling people that we moderate comments and

1 not to post their private information. We're very
2 clear. We have 153 videos up here and this one is how
3 to assemble a disaster kit, which is part of our
4 public mission. We actually have a public mission to
5 tell the public about disasters. One of our
6 successful videos was during the ice storms in
7 Kentucky. We were able to shoot a video quickly in
8 the field and put it up on YouTube so that State and
9 local Governments, when their power came back on could
10 learn how to apply for our public assistance program,
11 which gives money to State and local Governments. We
12 were able to direct them right to the YouTube page and
13 they were able to see what they needed to do because
14 Kentucky usually doesn't get aid from FEMA. So, they
15 needed to know how to do it and do it quickly so we
16 could get money on the street. So, this is very
17 important to get things out there. Also to get
18 information to the public on what we do because a lot
19 of people don't know what we do. They think that we
20 have all of these black helicopters and concentration
21 camps. We get a lot of comments on our YouTube page
22 about that. We moderate those out. For some reason

1 they're all over the place.

2 We also, to get around the persistent cookies
3 rule that I know you guys are also familiar about, we
4 created a multimedia site on our .gov site, which
5 mirrors what's on YouTube. All the same videos that
6 are posted on YouTube are posted on here. It's --
7 compliant and you can embed videos right to your
8 Web page if you want to. You can download the video or
9 you can download transcripts. This is on the .gov
10 site and we built it ourselves so we control
11 everything that's on here. We also have videos,
12 photos and audiocast, as well. So, we were able to
13 get around the persistent cookies issues since we
14 don't embed from YouTube to our .gov site, we take it
15 right from our multimedia site. We also allow anyone
16 in DHS to use this feature if they want to.

17 Then we started using Twitter. For us Twitter is
18 actually a very important tool. This is our FEMA
19 focused site and right now we're talking about disaster
20 declarations for Missouri. But we can also use this
21 to send brief 140 character messages, like "Hurricane
22 coming, get out. Shelters are located at. Ice drops

1 are located at." So, for us since you can get Twitter
2 on a cell phone, it's very helpful in a disaster. One
3 thing we did was our regions, we have ten regional
4 offices and each of them has a Twitter account. This
5 is our Region Five. They're located in Chicago. So,
6 they're Twittering different things that's in our
7 Region Four, who's located in Atlanta. Atlanta is
8 obviously very interested in hurricane preparedness
9 right now, where Region Five is a bit more interested in
10 flooding. So, they're discussing flood issues. We
11 also have an account for USFA, which is United States
12 Fire Academy to discuss training and push out training
13 information for fire fighters. So, we're using
14 Twitter at a regional level to make sure we get that
15 information so if you live in a particular region, you
16 can sign up for the regional Twitter feed and get it
17 on your cell phone if there's no power. So, for us in
18 a disaster we can get information to the public
19 quicker. We mirror everything that we put out on
20 twitter on our fema.gov site, as well.

21 Next, our programs decided that they had ideas
22 about using Web 2.0, too. One of our programs, our

1 mitigation program with our building sciences they do
2 a lot of publications for how to build structures that
3 are safe for disasters like hurricane safe buildings
4 and earthquake safe buildings and they wanted to put
5 their publications on Google Books. So, we negotiated
6 with Google Books and got an agreement and we have
7 about five books up there, we're working on it now and
8 these are downloadable, searchable, and printable in
9 full version on Google Books. We also have a library
10 on fema.gov where you can get the same information,
11 but this way it's in the Google search algorithm so it
12 comes up on Google when you start to search for these
13 things. We're working on doing things like adding our
14 logo and stuff, but this is a work in progress.

15 Then we recently started our Facebook page. We
16 haven't officially launched this yet. We're doing our
17 MySpace page at the same time. Even without
18 officially launching it, we already have over 1,200
19 fans. We're not sure how that happened because we
20 haven't told anyone about it, but it's there and you
21 can see it's mostly our press releases. Most of the
22 people commenting are actually our employees, believe

1 it or not on their own time. We also put out
2 disclaimer and privacy policy right in the info
3 section and we also put it on our discussion boards.
4 Not that anyone has posted anything, but we put it
5 right here so it's in several places on Facebook
6 because we wanted to make sure that we were telling
7 people what our policies are using these tools. It
8 was very important to us. We also, as you can see,
9 all of our social media tools has this FEMA-In-Focus
10 branding on it. We wanted to brand everything so
11 people knew that was our information. There are a lot
12 of people pretending to be us and in a disaster we
13 didn't want people giving out misinformation and
14 claiming it was us. So, we wanted to have a branding
15 so that people would validate our information and know
16 that this was official and they could trust it. So,
17 that was very important to us.

18 As we moved on we noticed that there was a need
19 for more governance in policy. So, we created the
20 FEMA Policy Working Group. What we did was we brought
21 together our FEMA programs, records management, IT
22 security, legal, IT, External Affairs, who is our

1 Public Affairs Office and the Office of Policy. We
2 just finished the first draft of our policy, we're
3 about to send it to the Policy Working Group for
4 finalization and we may have it signed in a month or
5 two. It all depends on what happens as we're in the
6 middle of hurricane season right now. So, everything
7 kind of gets halted if there is a big disaster. So,
8 we'll see what happens. But we are working on that
9 and that's going to be some guidelines on how you go
10 about using social networking and social media. What
11 we decided in these groups was that there were three
12 uses for Web 2.0 within FEMA. One is our internal and
13 that's a picture of our Office of Chief Counsel ESW
14 system, which is Enterprise Shared Workspace. It's a
15 SharePoint based system and we're actually very proud
16 the Office of Chief Counsel who was the first to in FEMA
17 to get their own SharePoint, official SharePoint
18 site. No one believed the lawyers would be first, but
19 we begged. So, we're launching all of those for all
20 our offices and we're working on that project, our
21 external, which I just showed you and our third group,
22 which we call "Situational Awareness."

1 For us and our mission, it's very important that
2 we share information with our State and local
3 partners. Now, this is not something we want the
4 public to actually be aware of. The public does not
5 need to know what the first responder is saying up the
6 line, but for us we need to share it with the Federal
7 agencies we work with, with their State partners and
8 their local partners and also in training. So, we
9 need to start working on this kind of middle level
10 between external and internal and that's our next
11 project. So, we've been talking about a bunch of
12 things for that, using a Twitter-like feed on our
13 servers, but we know that there are a lot of issues so
14 we're going to have to go through those issues before
15 we can launch anything.

16 We've also developed what's called a Web 2.0
17 strategy and the first thing is that you need to have
18 an appropriated need. We're all using appropriated
19 funds and I'm going to talk about the legal issues
20 tomorrow, but you still need to identify that with
21 your mission needs. If you have a public facing
22 mission, social media is a great tool to use for your

1 public facing mission. But if you don't have a mission
2 need, you can't just do it because you still it's
3 cool. You then have to identify the tool that you're
4 going to use. Then you need to bring in all those
5 people who have issues with you using the tool, IT,
6 security, legal, privacy, records management. We're
7 developing our records management schedule for Web 2.0
8 tools because we knew there was a records issue and we
9 can't delete anything. Then you develop a plan to
10 address these issues and then you implement with your
11 standard operating procedures. We use a lot of SOP
12 hoping to make sure that we keep within our lane and
13 keep everything legal. Our goal is to engage the
14 public and do it right.

15 Looking forward, we want to work with our
16 partners, our non-government organizations such as the
17 American Red Cross who we're statutorily required to
18 work with, our State and local partners with our
19 regions, with our FEMA programs, but we want to work
20 together to develop tools to support our mission and
21 we want our employees to use these tools. We want
22 them to use social media to do their jobs better and

1 so we can do our mission better. And that's about it
2 for me.

3 MODERATOR SAND: We have some time now before the
4 break, if you have any questions please lineup in
5 front of the open mike and our panelists will help
6 you.

7 AUDIENCE PARTICIPANT: Hello, I'm Jeremy Duffy
8 from the Interagency Support Staff and it's great that
9 everybody is looking at using current technology. I
10 think that's critically important and it vastly
11 increases our ability to do our job and do it well,
12 but what about the issue of people giving away too much
13 information online, giving away details of the
14 organization and themselves? Most notably things like
15 itineraries, which is nothing short of an
16 assassination plan in the wrong hands. How are you
17 guys training your people who are using these
18 technologies on operation security principles and
19 keeping their information to themselves?

20 MR. RICHE: The Department of State had long
21 standing rules regarding what information is shared
22 from the Embassies and as far as who is allowed to be

1 pictured on a Web site, it's only the Ambassador and
2 the second in charge. The rules are pretty extensive
3 regarding what can be shared.

4 MS. TELLER: The same is true with the Department
5 of Defense. Operational security measures still
6 apply. The way you communicate may be different, but
7 what you're supposed to communicate or what you're not
8 supposed to communicate is not different. One of the
9 things we're doing is working with the Defense
10 Information Schools to train Public Affairs officers,
11 as they're being trained as public officers how to
12 deal with these kinds of tools and get them to
13 incorporate this thinking from the outset. We are
14 influencing curriculum and developing curriculum.

15 MS. CRAMER: We're adding in our internal policy
16 about Government employees not disclosing nonpublic
17 information. So, that's going to be in our internal
18 policy, as well. Plus the only people who have access
19 to our sites right now are our Public Affairs officers
20 who have been trained. We don't let our regular
21 employees use our official sites. Now, if they post
22 something in their personal capacity, we go after them

1 using the ethics rules.

2 MR. BURNS: With TSA we have regular training on
3 -- and sensitive information. Everything on our blog
4 is moderated. So, anything that comes through on our
5 blog or anywhere else we take a close look at it to
6 make sure they're not revealing any sensitive
7 information.

8 AUDIENCE PARTICIPANT: Hello Leo Scanlon from the
9 National Archives. This is kind of to Victor, but
10 maybe to everybody. You told a story of the risk
11 acceptance that occurred at the meeting that you got
12 fired at. And while that's exemplary I don't know it's
13 common place and we're currently, I think in a risk
14 avoidance mode with respect to managing information.
15 Whether rightly or wrongly, it's driven by statute and
16 what we think is public perception. Again, whether
17 that's true or not we treat it as though there's a
18 zero tolerance for data loses and that's a huge cost
19 driver and that's a big limiter on what we can think
20 about and what we can try to do. My question is it's
21 great all this stuff is happening is, but who's going
22 to bell the cat such that what you described occurs

1 more often than not or actually gets written somehow
2 into the statute? So, what's coming up in Congress
3 right now doesn't look good statutorily. It's more of
4 the same, maybe worse. I think that's something that
5 would be very helpful too. I wish I'd thought of that
6 when Vivek Kundra was here, but maybe the rest of the
7 panel have some thoughts about where that's going to
8 go because I see it as a major barrier to turning the
9 corner on this and I'd like your thoughts on that.

10 MR. RICHE: Risk acceptance and risk management
11 is definitely something that we've talked about for
12 quite some time. It's a matter of education and you
13 have to sit down with the people one on one. This is
14 sort of my philosophy. If you get a group of people
15 together you're not going to be able to really delve
16 into their specific pain points and so you have to go
17 ahead and meet with the records people one on one,
18 meet with the privacy people one on one so that they
19 can speak freely and deal with their issues and
20 concerns and then build a consensus and that's
21 basically what we've been doing.

22 MS. CRAMER: From my prospective our goal is to

1 bring those people into the conversation very early so
2 that's why we setup our working groups so that we're
3 addressing these issues. One of the key issue
4 spotters, being in legal, that we have the overview to
5 see a lot of the issues, so I do a lot of issue
6 spotting and because we're very small we can then
7 bring those people in one on one and work out the
8 issues and we do this on the project by project basis.
9 So, we address the issues before we go ahead and
10 launch.

11 MS. TRUDEAU: I actually think the issue you've
12 raised is probably the most fundamental issue when we
13 talk about moving to a more innovative kind of
14 Government. If we do not find a way to create the
15 enabling infrastructure for some level of risk taking,
16 we'll never see true innovation. It's one area where
17 the National Academy of Public Administration, I think
18 can play a helpful role. We started something about a
19 year and a half ago now called the Collaboration
20 Project. The intention in doing that was to create a
21 safe space where agencies could come together and
22 share information about what they were doing, what

1 works. I've heard so far this morning some great
2 examples of policies that are being developed and
3 means that are being found to get us through what on
4 our end, we don't call them barriers anymore, but
5 they're gates. You have to pass through those gates
6 and there are certain things you have to have
7 accomplished in order to pass through those gates.
8 There are a lot of agencies and departments that are
9 figuring this stuff out, at least at a micro level and
10 if we could get together and share all of that
11 information and also use a good Government
12 organization like the National Academy to be able to
13 let agencies take a stand that they wouldn't otherwise
14 take on their own, but maybe could take a
15 collaborative stand on a particular issue where some
16 of the laws may need to change, where statutes need to
17 be updated I think it would be of benefit to all.

18 MR. AMES: I think I would agree with everything
19 that was said. Having spaces like the Collaboration
20 Project, GovLoop is another online source to connect
21 people who are doing this stuff throughout the
22 Government is a good thing because honestly I think

1 like social media this is going to have to be ground
2 up effort. Those of us who are sort of stumbling into
3 it and encountering the obstacles are really going to
4 have to build momentum and be able to make a case for
5 why it's absolutely important for Government to be
6 playing in this medium and therefore what the next
7 phase is. So, legislative and policies are going to
8 be needed in place to allow for that sort of
9 innovation to occur and to have some level of risk
10 taking and therefore some willingness for some
11 projects to fail so that others can succeed. I think
12 it's just going to be a culture shift that's going to
13 have to be built from the people in this room.

14 AUDIENCE PARTICIPANT: Good morning, I'm Michael
15 McGrath I'm from Gemalto. I have a question for Jodie
16 specifically with FEMA's use of Facebook and those
17 types of social networking sites. Security on some of
18 these sites are lacking, poor at best my own personal
19 Facebook account has been compromised where blasts
20 have been sent out to all of my friends on Facebook,
21 some sort of a virus. From FEMA's standpoint, I'd
22 like to know, well I can see a major panic potentially

1 happening if a blast came out from FEMA through some
2 sort of a virus or whatever that said there was a
3 tsunami headed towards California. All the people on
4 the beach seeing this tsunami would be heading for the
5 hills real fast, so I just want to know if FEMA has
6 looked at that and taking any precautionary steps
7 before launching the Facebook site?

8 MS. CRAMER: Basically, right now we're just
9 using our Facebook site to push out our press releases
10 already. So, we're just pushing out information we
11 already have on our .gov site and we've decided to
12 make our .gov site the official bible of our
13 information so we always link back to our .gov site
14 and link back to our links so you always link back to
15 .gov. So, our way to deal with it is that the links
16 go right to .gov we don't post the whole story on
17 Facebook. So, you couldn't get the full message there
18 you still have to come back to our .gov site to get
19 the official word.

20 AUDIENCE PARTICIPANT: Hi, Liz -- I have a
21 question that sort of goes along with that for Jodie
22 and everyone else. You had mentioned the importance

1 of branding and having that developed so that fake
2 messages aren't going out. What kinds of tools are in
3 place to prevent the imitators, the people that are
4 acting as FEMA, but not?

5 MS. CRAMER: That's me. One of my other duties,
6 which seems to get added to everyday, is I am on seal
7 patrol and we're going to talk this a bit more
8 tomorrow during the legal panel. I write all the
9 letters to everyone telling them if they're using our
10 seal improperly and we actually had a great success a
11 few months ago. We had a company that was sending out
12 emails to our people that said, "Buy FEMA batteries
13 and buy FEMA flashlights." And it went around. We
14 sent them an email telling them please stop, you're
15 using our name, you can't do that, it implies
16 endorsement, etc. They didn't stop. We went and
17 looked on their site to send them a certified letter
18 and low and beyond they were on GSA schedule. So, I
19 called up GSA and I said, "One of your contractors is
20 sending out these emails." I sent a copy of the email
21 to GSA and asked the contracting officer to tell them
22 to stop. The contracting officer called them and they

1 verbally refused to stop. So, the lawyer for GSA
2 wrote a letter and finally they agreed that they would
3 no longer use our name because they threatened to
4 terminate the contract. So, we do go after people who
5 use our seal improperly. We're going to talk about it
6 a bit tomorrow, but there are some acts in Congress to
7 protect certain seals and some agencies have that.
8 DHS does not have a seal act. There was talk about it
9 at one point, but it never went through and that will
10 be one of those things that could help us if there
11 were criminal charges for improperly using our seal,
12 but we do go after them at least to annoy them, if
13 nothing else.

14 MS. TRUDEAU: So, this is a huge issue that we've
15 heard from many, many folks across Government. People
16 are struggling with it just purely from a bandwidth
17 issue. Jodie can only spend so much time searching
18 online for companies and other organizations that are
19 improperly using the seal or the brand of the Federal
20 Emergency Management Agency (FEMA). So, I have two
21 things to say on this. One, is that one of the best
22 things you can do to combat inappropriate use is have

1 a strong branding effort around your own appropriate
2 use and make sure that you are undertaking efforts to
3 get communications out to the stake holders who need
4 that information through all the channels that are
5 available to you and if you have a legitimate
6 appropriate sort of messaging strategy your stake
7 holders will learn over time where to go in order to
8 get the right kind of information.

9 Secondly, at our last meeting of the
10 Collaboration Project we had a panel of legal folks
11 from across Government and this was an issue that
12 actually Rashad Hussain, who is Deputy Counsel to the
13 President asked if we would take on at the
14 Collaboration Project level as a first step in looking
15 at some of these challenges in the legal environment.
16 There was a question of advertising and inappropriate
17 use. So, if anyone in the audience is interested at
18 all in participating, we're putting a meeting together
19 around that issue specifically. So, just see me
20 afterwards.

21 AUDIENCE PARTICIPANT: Hi, I'm Danielle Citron
22 from Maryland Law School. A lot of the tools that you

1 talked about were very much in sort of the broadcast
2 bottle that Maxine talked about, very twentieth
3 century. I wonder if in this panel, you guys will be
4 talking about how you're using these tools in a much
5 more collaborative way rather than just comments,
6 which seems like what we talked about -- so long ago.
7 I think that'll be really interesting for our audience
8 to hear.

9 MR. RICHE: Yes. The Connect site is actually
10 suppose to be a collaborative site where people come
11 in and they start their own conversations. That's the
12 idea behind it. It's not just for us to go ahead and
13 to talk about what's going on at the Department of
14 State, it's for people there to generate their own
15 topics and talk about them.

16 MS. TELLER: At some of the Blogger Roundtable
17 Program that's what happens, the bloggers are talking
18 to one another. It's catalyzing new relationships
19 between bloggers, as well.

20 MS. CRAMER: Our collaborative site is on our
21 external site and that is a complete collaborative
22 site using SharePoint and we're working that

1 internally. We're also working on the collaboration
2 in our situational awareness. We feel that's a more
3 important use of our efforts right now than externally
4 for obvious reasons because it's more important for us
5 to communicate with our State and locals during a
6 disaster than it would be with the public to be more
7 collaborative right now. So, we're putting our
8 efforts there.

9 AUDIENCE PARTICIPANT: Liz Blumenfeld from the
10 Library of Congress. We are a cultural institution
11 and so we are always trying to reach out to the public
12 and draw them in. So, we are interested in working on
13 all of these social media opportunities. One thing I
14 haven't heard today is a discussion of children and
15 protecting their private information. As you know the
16 laws are more strict with regard to that and I'm
17 wondering has nobody discussed it because it's just so
18 built in to everybody's thinking that they're aware of
19 it or is it that you're not seeking to reach out to
20 children? I'm thinking of Twitter, for example. So
21 many kids have cell phones, they're under the age of
22 13, I'm curious as to folks thinking on this and what

1 ideas they have to maintain the protection of
2 children?

3 MR. RICHE: There was another video contest that
4 the Department held called, "My Culture Plus Your
5 Culture Equals" and then people submitted videos and
6 we had two categories, one was adults and one was
7 targeted to 14 to 17 year olds and people are not
8 allowed to sign up to sites if they're under 13. So,
9 we are very aware of that and we definitely want to
10 reach a youth audience. If you go to the Connect
11 site, connect.state.gov, you can go ahead and take a
12 look at some of the past winners and the young people
13 that went ahead and won domestically, as well as,
14 overseas. We're definitely trying to reach a youth
15 audience.

16 MS. CALLAHAN: With regard to engaging children,
17 I worked a lot on Children's Online Privacy Protection
18 Act in my former life. So, for these sites that are
19 here the standard is either that it's a children's
20 site. So, if you're collecting personally
21 identifiable information about children on a
22 children's site, you assume that all people on that

1 site are under the age of 13. The alternative is, if
2 it's a general audience site, which a lot of the
3 Government sites are, in that circumstances only if
4 you have knowledge that the person is under the age of
5 13. So, in that circumstance it goes to what Vivek
6 Kundra was talking about before, which is what type of
7 information do you need to collect about somebody in
8 order to engage in a dialogue with them. If there is
9 somebody who is under 13 on FEMA, but is engaging in a
10 typical dialogue with them and they don't know that
11 they're under 13, in that circumstance FEMA shouldn't
12 ask, "Hey, what's your age? What's your social
13 security number?" It's data minimization consistent
14 with the fair information practices. So, I think to a
15 certain extent Liz, maybe this issue isn't as in front
16 of these types of sites because they're probably
17 mostly general audience while the library does do
18 target under 13 approaches. She's absolutely right in
19 addition to all the other legal and policy issues we
20 have to address we do want to think about if we're
21 engaging with under 13 and we know it, then we need to
22 make sure that we have the appropriate policies and

1 procedures consistent with law.

2 MS. TELLER: One of the questions I get asked a
3 lot is, who do you let participate in the Bloggers
4 Roundtable discussions? The answer is anybody who
5 wants to, but they have to be screened first. We just
6 need to know who they are. We have not excluded
7 anyone. To date we just want to be able to take a
8 look at their blog and say, "Oh yeah, this is a
9 blogger, they write about military stuff." They don't
10 have to agree with us. They don't have to have
11 political bent, but we want to see who they are. So,
12 yes I guess if they were a child I guess that would
13 raise that issue, it hasn't to date.

14 AUDIENCE PARTICIPANT: I'm Elizabeth Hochberg and
15 I'm General Counsel Office at GSA and Jodie I am your
16 friendly trademark sheriff. To any of you in the
17 room, I actually brought up this question previously
18 to Lena and Jodie over at a NAPA meeting. Branding on
19 the Internet and the affirmative duty, actually not a
20 defensive but an affirmative duty that trademark
21 holders have to follow our brand and be proactive in
22 going after trademark violators and not simply

1 reactive. So, I wanted all of you to know that GSA;
2 hello, army of one here, are spending nearly sometimes
3 50% and sometimes 100% of my time using software and
4 other available tools to go after the infringing
5 Web sites and do what I can to send out hundreds of
6 cease and desist letters. So, I just wanted to say
7 trademark sheriff at your service, glad to help.

8 MS. TELLER: One of the things that we talk about
9 is this being sort of an issue of national security.
10 You have to go and go onto the various Websites and
11 secure your Twitter name and secure your Facebook name
12 and things like that so that somebody else doesn't and
13 if you don't, if you're not taking responsibility
14 actively somebody else might do it for you and they
15 may not be your agency and then you definitely have to
16 get your legal folks involved.

17 MS. CRAMER: It's the same with domain names.
18 We're picky about what we go after. We had a couple
19 of domain names doing fema.cn, whatever and we
20 actually talked to TPL and they told us that we
21 shouldn't bother going to the World Intellectual
22 Property Organization and get our names back unless

1 they started using them, but we're actually very
2 active. We look for people using our name. We just
3 shut another one down that was using FEMA and actually
4 copied our page. So, we have had success in going
5 after people. I don't have all day to do it and I
6 don't go looking for it, people tell me. Our people
7 are out there a lot and we have a lot of people who
8 send it back to us. They're very good about letting
9 us know when someone uses our name. So, our employees
10 are pretty good at bringing it back to us so we can
11 take action.

12 AUDIENCE PARTICIPANT: For one of the screenshots
13 I saw from some of the Government run sites, YouTube
14 channels I kept noticing something saying, "moderated
15 comments." I was wondering how you're handling any
16 sort of free speeches that have come up about that
17 operationally from policy and any concerns about
18 creating a perception of censorship around those
19 moderated comments.

20 MS. CRAMER: We put really clear outlines of what
21 we were going to moderate. It's abusive language,
22 privacy information, vulgar comments, I can't remember

1 what else I wrote, but there's a list of topics. We
2 made a policy decision that we were not going to
3 censor anyone who disagreed with us if they were
4 constructive comments, especially on YouTube. For
5 some reason its YouTube not anything else. We get a
6 lot of comments on black helicopters and concentration
7 camps. It's really just conspiracy theory and it's
8 really off topic, but we have posted comments. We
9 don't post them directly on our channel, we post them
10 on the video channels themselves, but we have posted
11 things that disagree with us. We still have other
12 comments because of records management, we can't
13 delete them right not. If someone wanted to -- them
14 they could get, but they're really everything that
15 we've deleted or haven't posted. They've been very
16 crazy stuff and off topic and that's part of our
17 policy comments in there, it says off topic.

18 MR. RICHE: If I could just add that at the
19 Connect site, the social networking site we also have
20 very clear terms of services. We have a community
21 manager that manages the site day in and day out. We
22 just recently issued a contract that's going to

1 monitor the site 24 by 7 to make sure that nothing is
2 put up there that's inappropriate. When we have taken
3 people off it actually goes very high level in the
4 bureau that supports the Web site or the community.
5 So, it's something that we have thought about and we
6 monitor it actively.

7 MS. TRUDEAU: Sometimes it gets a little dicey.
8 I don't know if anyone has been paying close attention
9 to the open Government dialogue three phase process
10 coming out of the White House and the Office of
11 Science and Technology policy that's intended to
12 generate recommendations for input to the open
13 Government directive that is hopefully coming out in
14 the coming months. The National Academy hosted the
15 first phase of that process. The folks at the White
16 House came and asked for our help in hosting that
17 primarily because there were some I guess concerns
18 about the White House's ability to host the first part
19 of that versus the National Academy's ability to host
20 it. We were using in working with the White House
21 selected a platform called, IdeaScale, that's a free
22 service. So, that opens up a lot of issues as you

1 know in this audience. So, we hosted that first phase
2 and for the first week or so it was pretty civil
3 dialogue. It was well moderated. We had clear
4 moderation policy and then a Web site called, World
5 News Daily got hold of this vehicle for providing
6 their comments to the White House and promoted through
7 their Web site the birth certificate controversy,
8 wherein hundreds of people, thousands of people
9 actually came to the site to post ideas, asking the
10 President if he was really interested in transparency,
11 to release his birth certificate. Well, according to
12 our moderation policy, our moderation policy gives us
13 some leeway at the National Academy in terms of what
14 we choose to leave up and what we choose to take down.
15 Anything with obscenity in it, anything with
16 personally identifiable information came down right
17 away. Really, the question is a request for
18 information from the Government does have a link,
19 however tenuous to questions around openness and
20 transparency and so the question we debated internally
21 was whether to take this information down or leave it
22 up and we erred on the side of leaving it up. When

1 people submitted ideas that they then couldn't find,
2 even though we hadn't taken them down we were accused
3 loudly of censorship and being the tool of various
4 nefarious entities, but anyway. At the end of the day
5 when you're really trying to balance the utility of a
6 site like this to achieve the objectives that you want
7 to achieve with the desire to handle all comments in a
8 very evenhanded way, it raises a lot of issues. We've
9 learned a number of things coming out of that and
10 we're producing what we're calling a sort of an
11 observations or a lessons learned report that we'll
12 have available in the next week or so and I'll make
13 sure that it gets added as a link to the Web site at
14 DHS so that you can all download it if you'd like.
15 One of the things that is really important, I think
16 that Jodi mentioned is having a parking lot or
17 someplace where you can take things that are not
18 central to the conversation and place them in a spot
19 where people can see that they haven't been deleted,
20 but at the same time it leaves your main part of your
21 site open to trying to achieve the objectives that
22 you're really trying to achieve. It's very, very

1 helpful.

2 MODERATOR SAND: I want to thank our panelists
3 for doing a great job on this first session. We're
4 going to take a 15 minute break. It's a little short
5 now, so maybe a 12 minute break and come back at 10:45
6 for the second session. We'll have some more
7 opportunities for questions after that. Thank you.

8 (Recess from 10:30 - 10:45)

9

10 Panel 1: How is Government using social media?

11 MODERATOR SAND: If you didn't find the restrooms
12 this time, you'll have another opportunity, there's a
13 set along the hallway here to the left and then down
14 and to the right.

15 And also there's a list of restaurants and places
16 to eat in this area.

17 There's paper on the table out there, again I
18 encourage you to use that fancy technology we're
19 talking about and save the trees, so please work with
20 each other, socialize, network eyes and find a place
21 to eat around here during our lunch break.

22 We're going to pick up again with the remaining

1 panelists here, we have three more, then there will be
2 another opportunity for questions 15 minutes before we
3 end, so it would be around 11:45, we'll end at noon,
4 that will be lunch and then we'll start up again with
5 the Workshop at 1:30, thanks again and here we go.

6 MS. TRUDEAU: Thank you. So I'd just like to
7 start off with a couple of high level slides, it - -
8 given the fact that this is a largely Government
9 audience it bears mentioning that this is how the
10 majority of the world sees their interaction with
11 Government in an attempt to gain Government services,
12 you know, I love the way Vivek put it this morning
13 when he talked about the fact that we replicated on
14 line our, you know, maze of bureaucracy and it's true,
15 it's really difficult for a lot of folks to navigate
16 and it feels to a lot of people like a very closed
17 system, so what do we do about that? This is supposed
18 to be a Government by the people.

19 The challenge is that in addition to the fact
20 that we have a lot of these stovepipes, there are also
21 problems that cut across Government and go outside of
22 the boundaries of Government more than ever before.

1 The challenges that we're facing require people to
2 work across a lot of systems and in an environment
3 where there is a lot of regulation, those legal and
4 policy issues cannot be ignored. Often times we have
5 a desire to move forward quickly and see people in our
6 privacy offices, or offices of general council as
7 people who are throwing up roadblocks when that's not
8 the case, these are people who are required to protect
9 the Agency, to adhere to statute and policy and those
10 policies are in place for good reason.

11 I don't see Peter here right now, although maybe
12 he took a different seat. Peter Swire was sitting
13 here just a short while ago, there's his bag.

14 (Laughter)

15 MS. TRUDEAU: And Peter was part of the
16 Transition Team, specifically he worked on a team
17 called the Government and Information Technology
18 Reform Subcommittee or Transition Team and folks from
19 that Team were over at National Academy Offices for a
20 couple of meetings when they were working through the
21 process of trying to move Change.gov to Whitehouse.gov
22 and understand what functionalities they could really

1 employ and it was really interesting, we had a great
2 conversation about persistent cookies and our
3 inability to, you know, use that particular
4 functionality to great affect the way that the private
5 sector does just as a matter of course and Peter sort
6 of sheepishly raised his hand at the end of the
7 meeting and said, well, I have to confess that I'm
8 actually one of the authors of the persistent cookie
9 memo and now that we're actually trying to get things
10 done in a way that is responsive to the needs and the
11 desires of the American people, you know, you realize
12 there are constraints in place, so.

13 But, you know, interestingly, as well, I think,
14 and as Maxine very rightly pointed out, the majority
15 of the challenges aren't technology challenges, the
16 technology can do anything you really want it to do,
17 it's the management question and the policy question
18 that has people confounded right now.

19 The technology enables more transparency
20 collaboration and participation than ever before and
21 that allows people to engage in Government in an
22 entirely new way.

1 The involvement that we saw in the last campaign
2 and the groundswell of interest and engagement in
3 issues that are, you know, Government issues,
4 traditionally seen as Government issues is, it's
5 overwhelming right now for a lot of agencies that are
6 seeing people seek to get engaged in new ways, the
7 demand is really there. The challenge for us is if we
8 don't, in our position in Government, do something
9 about engaging with those people and satisfying that
10 need, whether it's a demand for more information, or a
11 desire to get involved in the decision making process,
12 or a desire to actual collaborate around the delivery
13 of Government services and people will go and do that
14 anyway, and they may not involve us and so this is
15 just a screenshot from Google Flu. CDC has done great
16 work around, you know, using Web 2.0 technologies and
17 Social Media to really get information out to people
18 where they live, but, at the same time, you know,
19 Google Flu is a pretty - - is a pretty good tool, as
20 well, and so the question always is if we don't play
21 in that space, or if we don't play quickly enough, or
22 effectively enough in that space, what's going to

1 happen around us that might completely remove our
2 ability to influence the direction that that
3 information takes, or that that, you know, public
4 engagement takes.

5 I just want to stop for a second, this is sort of
6 an old slide that I use and I haven't had it out in
7 awhile, but I wanted to put it up here because we
8 tend, I think, to think of Web 2.0 in a very narrow
9 way from this perspective. We always think, or we
10 first think, maybe, about the connection between
11 Government and citizens. And the reality is, there is
12 a whole lot that we can get done by enabling
13 collaboration inside government, things that can
14 happen inside the firewall that might be a little bit
15 of an easier lift, if you're first starting out, that
16 can
17 - - really there's a lot of low hanging fruit, there
18 are a lot of efficiency can be gained, a lot of
19 agility can be gained as a result of that and so I
20 just wanted to talk for a second about this construct
21 we've used for awhile, where we talk about technology
22 enabling people to connect with their front line, we

1 have TSA here, I'm sure they'll talk about Idea
2 Factory, which is just, to my mind, one of the best
3 examples in Government of engaging your front line
4 workforce and helping achieve the mission of the
5 organization. Engaging stakeholders, Virtual Alabama,
6 I'm sure with all the DHS people in the audience,
7 we'll have a really good conversation about
8 applications like Virtual Alabama, which increased,
9 vastly increased our situation on awareness, but if
10 you're going to talk about privacy, I mean, bringing
11 all of these different data fades together in a way
12 that provides the situational awareness that a Virtual
13 Alabama provides raises huge questions about
14 Government as Big Brother. Downing Street E
15 Petitions, you see a lot of this in the U.K. and peer-
16 to-peer, you know, Intellipedia is a great example,
17 and these are just - - these are just a few examples,
18 I'll scroll through the page shots, the screen shots
19 here. There are a few examples that we use, they've
20 been around for awhile, but they're really good
21 examples of the types of things we're talking about.
22 There are many, many other examples that are more

1 recent, as well.

2 I've mentioned the Collaboration Project and I
3 wanted to throw a screen shot up here because if you
4 go to, there's a tab on here that says Content,
5 there's a lot of content in this site that's really
6 available to anybody who'd like to use it and what we
7 did during the transition period, because we have a
8 lot of demand from folks in our membership, was to
9 create a list of a number of the different gates we -
10 - as I said, we used to call them barriers, but gates
11 that we've been talking about, different issues
12 related to law or policy that, or for that matter, you
13 know, culture and operations that serve to provide
14 challenges to people who are trying to implement Web
15 2.0 approaches.

16 Privacy is up there, if you click on Content and
17 you go to, I think the tab is called Legal Issues, but
18 I'll make sure the link is provided. You can find
19 information on Procurement Law, you can find
20 information on 508 Compliance, you can find
21 information on Privacy, on Security, on Data
22 Authenticity, a number of these things it's pretty

1 well organized and it's organized in a Wikipedia like
2 fashion, so there's a brief overview of what the
3 nature or substance of the challenge is, and then a
4 number of links to additional information.

5 This entire site is built on a Wiki platform, it
6 is confluent, so if you see something that you think
7 is wrong, all you have to do is register on the site
8 and go in and edit it and we'd be happy for you to do
9 that.

10 As well, there's a tab here that says Cases, you
11 know, one of the things I think that we could do a
12 better job of in Government, and it would help with
13 this culture that we have of a reluctance to take any
14 risks. If you are interested in solving a particular
15 problem in your organization through the use of these
16 new tools and approaches, you can probably find an
17 example of where it's been done before on this site.
18 There's 60 or 70 cases up there right now that span
19 Federal, State, local and non-governmental, but all
20 related to government service delivery and policy
21 development types of issues. If you
22 - - if you go on there you'll see that the cases that

1 we have up there are organized as addressing four
2 fundamental questions, what - - the first question is
3 what business problem were you trying to solve? The
4 second is what approach did you use? The third is
5 what lessons did you learn? And the fourth is, what,
6 if any, results were you able to document? And what
7 we're doing with that database of information that
8 we've compiled, and that we continue to compile, is
9 we're doing research on that to say, well, what kinds
10 of business problems lend themselves to which types of
11 solutions? What's proving to be most effective?
12 Where are we seeing the highest return on an
13 investment? That's the kind of data we want to be
14 able to get to because we think that makes the case
15 for using these sorts of approaches.

16 Again, you know, a Wiki enabled site, if you have
17 a case you'd like to put in there, I really encourage
18 you to do that, all you have to do is register on the
19 site, it's free and add your own case study and then
20 you'll make that information accessible to others
21 across Government. The URL for that is the
22 Collaboration Project at org by the way.

1 I wanted to spend just a couple of minutes
2 talking about some of the things that we've been doing
3 at the National Academy in support of other
4 organizations. They've mainly been in the
5 collaborative brainstorming space when we've done, you
6 know, particular online, we call them dialogues and
7 the notion here is that if you time limit an online
8 conversation, and you enable people to post
9 information in many different forms, you build a
10 community of people who are passionate about the issue
11 you're dealing with, you enable them with some
12 functionality, like some simple voting and tagging
13 tools.

14 And then we also have this role called catalysts,
15 we like to bring into these conversations. One of the
16 benefits of being at the National Academy is we have a
17 group of Fellows about 650 people who are all very
18 accomplished in various fields of Public
19 Administration that we can access as a brain trust and
20 so between these experts and others who might be
21 outside of our organization we're able to bring
22 together sort of advisory panels of people who act as

1 discussion catalysts, who can go onto the site in the
2 middle of a conversation and correct misinformation,
3 or if they see a threat of discussion that's really
4 interesting and important, but it's petted off a
5 little, you know, throw a comment in to juice it and
6 really help to guide the conversation a little bit.
7 And the notion here is through these kinds of
8 brainstorming sessions, being able to produce an
9 outcome that government agency can act on, rather than
10 just having an electronic suggestion box that gives
11 you thousands of more ideas than you used to have, but
12 no real way to discern what, you know, how to organize
13 that, or what real recommendations are coming out of
14 it and we think built to methodology in a platform
15 that helps get at that.

16 Just a couple of examples, we held a dialogue for
17 the Recovery and Accountability and Transparency Board
18 on IT Solutions, that's a screen shot there, that
19 information is all still available, the dialogue
20 itself is closed now, but if you wanted to check it
21 out, the NationalDialogue.org, all the data that
22 people submitted as a part of that is still available

1 online and we produced a report in which I'll talk a
2 little bit more about in a minute, but just in
3 deference to Toby who loved to hear that we actually
4 have a stated Privacy Policy and Moderation Policy on
5 our site, but I'd highlight the fact that we do and
6 invite, I mean, there are so many people in this room
7 who are way smarter than me on this kind of stuff,
8 right? If you go to the NationalDialogue.org and
9 click on that Privacy Policy, I would love to hear if
10 you think it's any good. I've seen privacy policies
11 in a number of different sites and they vary greatly.
12 There's a struggle that we had internally between
13 keeping something in plain English and relatively
14 simple and actually being able to answer the mail in a
15 robust way on a privacy policy, so if anyone has
16 thoughts, I'm really open to hearing about it.

17 Our Moderation Policy, based on our most recent
18 experience with the OpenGov brainstorming session is
19 actually under review right now, we think we could
20 make it a little bit tighter, so we'll be coming out
21 with a new Moderation Policy soon, but this one here
22 that's listed on the site, I'm very, very happy to say

1 we saved a great part of it from TSA whose Blog,
2 Evolution Security is great and if we could have had
3 to delete them, you know, we really would have, but,
4 again, any improvements we're happy to consider.

5 We hosted, also, a dialogue on Health IT and
6 Privacy back in the fall, I wanted to reference this
7 one specifically, because of the connection to privacy
8 issues, in particular, you know. Health IT, I think,
9 that there's a broad understanding in America that
10 greater and more effective use of technology and
11 delivery of health care services is critical to
12 lowering health care costs, it's one of the major
13 planks of whatever is going to happen - - whatever is
14 going to be done in terms of our, you know, next
15 iteration of health care in America and the privacy
16 issues have been historically a showstopper, you've
17 had zero some gain, our whole debate on this issue has
18 been characterized by people either coming at it from
19 an IT perspective or a privacy perspective curving out
20 the space where they disagree and they arguing really
21 passionately about those areas of disagreement and our
22 view was we could maybe take this issue and

1 demonstrate the capability that we have with some new
2 tools and approaches, to instead of finding the areas
3 where we disagree and fighting over those, to build on
4 areas of consensus, to find that 70 or 80% where we
5 actually agree on things and see if we can use that as
6 a means to bridge the gap.

7 One thing that came out of this Health IT
8 Dialogue, the report is available on Scribed, by the
9 way, is a series of proposed principles, and these
10 were just draft principles that we provided in our
11 report that really stemmed from the conversation that
12 happened online over the course of 10 days, you know,
13 this isn't perfect, but it's a step forward and we'd
14 love to be able to take this draft set and put them
15 out to folks and let them see if they can improve on
16 them and maybe make that sort of principle based
17 approach part of our approach to Health IT generally.

18 I have a screen shot in here of the Open
19 Government Dialogue; I referenced a little bit earlier
20 the challenge of managing an online dialogue that is
21 freely available to anybody in the nation to
22 participate in for the White House on an issue that's

1 fairly high profile. You know there are challenges
2 that remain and there are ways to address those
3 challenges.

4 One of the things that I think a much better job
5 could have been done around in advance of this
6 brainstorming session was in building the community.
7 There were - - there was a desire to target,
8 particularly, people in the transparency, it's not
9 really an industry, but transparency organizations and
10 good Government groups around this and folks in, in
11 and around Government, as well. The fact of the
12 matter is, when you make available a means for people
13 to communicate with the senior most leadership of the
14 country, they're going to take advantage of that and
15 sometimes very small and very passionate groups of
16 people will form around particular issues and they'll
17 work together to put together, to put forward their
18 agenda, that's to be expected. The way to combat that
19 is to make sure that we do as much work in advance
20 knowing who we need to bring into this conversation to
21 build a really diverse and robust community, a
22 community that feels equally, strongly and

1 passionately about the goals that you may have for an
2 open conversation like this, because then if you have
3 groups come in and try and take the conversation in a
4 different direction, folks from the community can help
5 to moderate that themselves. Moderation in itself is
6 not something we always have to do as hosters of an
7 organization, that's something we can crowdsource.

8 But that's really all that I have and I look
9 forward to questions. Thanks very much.

10 (Applause)

11 MR. BURNS: Good morning. I'm going to start
12 things off with something just a little bit off topic.
13 This weekend, my daughter, my four-year-old daughter
14 knocked the crown out of my mouth and then went to
15 misplace it, so if you hear me random whistling up
16 here that's why, and if you see me talking like Eddie
17 Money, out of the side of my mouth - -

18 (Laughter)

19 MR. BURNS: I'm must trying not to reveal that
20 missing tooth right there, even though I am from South
21 Cincinnati, real close to Kentucky, that has nothing
22 to do with it.

1 (Laughter)

2 MR. BURNS: So with that's said, I feel better.
3 I'm glad to see FEMA's here because we share the same
4 kind of fan base out there, people love us.

5 (Laughter)

6 MR. BURNS: And we hear from them quite
7 frequently.

8 AUDIENCE PARTICIPANT: We're not going to say
9 anything about that.

10 MR. BURNS: Congratulations.

11 (Laughter)

12 MR. BURNS: But, you know, why start a blog, why
13 do you need a blog? And there's several different
14 reasons:

15 1) You want to humanize your workforce. And what we
16 were noticing is with the TSA on the checkpoint was
17 the passengers are coming through all day long, the
18 officers are screening them all day long, but there's
19 really not a whole lot of dialogue going on.
20 Passengers are sometimes afraid to talk to the
21 officers. The officers usually have work to do so
22 they're not really focusing on talking with the

1 passengers and a lot of times when they do talk to the
2 passengers, they're called Nazi's and things of that
3 sort, so they kind of shy away from that sometimes.

4 But we want to humanize the workforce with the
5 Blog, we want to show that, hey, you know, we are
6 human, we do care about what you have to say and we
7 want to listen to what you're saying and see if we can
8 make any changes. It's also a great way to bust
9 myths. With the TSA, I forget who said it, but it was
10 said once that the Coast Guard could miss a drug ship
11 full of drugs, weapons, whatever, and you wouldn't
12 really hear about it, but the TSA could, they could
13 miss a small Swiss army knife and it'd be on the front
14 page of the news and that's the truth and every day
15 there's fires to put out and sometimes these things,
16 these accusations that are made, are just that,
17 they're accusations and they're not really, there's no
18 truth to them, so the Blog has been a really good way
19 to fire back real quick and say, okay, so and so said
20 this, and this is what really happened. And what we
21 found with that is our Public Affairs Officers are out
22 in the field and our Public Affairs Personnel

1 Headquarters, once we do that, they get far or few
2 recalls from the media then what they would normally
3 get, because we've laid out all the facts right there
4 in the Blog, so it's really, we found out that the
5 media is using that and it's, not only is it getting
6 the word out to the media and the public, but it's
7 reducing the work load, our Public Affairs staffs.

8 Also, one of the most important reasons is
9 transparency, that's the whole big thing now, we want
10 to be more transparent with the public, let them know
11 what we're doing, the whys of why we're doing the
12 things we do, and that's also one of our biggest
13 challenges is being transparent because, you know, in
14 the government you have sensitive information that you
15 can't share and a lot of the decisions have been made
16 to declassify things as way above a blogger's pay
17 grade, so there's nothing I can really do sometimes,
18 other than to say, you know, we can't talk about it.

19 And if you've ever noticed on any kind of a
20 regular argument with somebody, if you tell them to
21 relax or calm down, that usually makes them more
22 angry. Well it's the same way in the blog world, if

1 you tell somebody, hey, you can't - - I can't tell you
2 anything because it's sensitive security information
3 that just infuriates them because they call that
4 their, you know, the SSI card, I just don't want to
5 answer it, so that's SSI. So if you have any
6 questions later that will be my stance, that's SSI.

7 All right, you still talk about some best
8 practices. Our Blog is linked on TSA.gov, which is
9 where we get a lot of our hits. TSA.gov gets millions
10 of visitors every year and are right on top of the
11 main Web page, we have a link to our Blog and we did
12 find out once that it was actually removed once for
13 just a period of like a week on accident and our hits
14 to the Blog went way down and so it's very important
15 if you're going to start a blog to make sure you link
16 it from your regular, your regular.com Web page.

17 We launched it in January of 2008. We've put
18 out, actually, close to 170 posts now, we try to post
19 at least once or twice a week. We're approaching a
20 million visitors right now to our Blog. We receive a
21 lot of comments. We've received almost 21,000
22 comments to all of our Blog posts we put out there

1 right now. Out of those we've only had to reject a
2 little over 1,200 and I'll talk about the
3 - - I'm rejecting the comments a little bit later, our
4 delete-a-meter was plugged earlier and I'll talk about
5 the delete-a-meter and what it does.

6 When the Blog was first launched we had more than
7 2,000 comments in the first three days, it was to the
8 point when we were moderating that you would clear 50
9 comments and then refresh the page and there would be
10 80 more waiting on you, it was crazy. And what had
11 happened was, the way the press handled this was, they
12 said, okay, you got a gripe with the TSA, they just
13 launched a Blog, TSA.gov and it was all over Fox, CNN,
14 everywhere, so prior to this people really didn't have
15 a venue to let TSA have it and, of course, there's all
16 sorts - - there's all sorts of examples out there of
17 why people wanted to let us have it and we knew that,
18 we knew that, you know, some of these were justified
19 and that's one of the reasons we want the Blog, we
20 want to hear what's going on out there and see if we
21 can make any changes.

22 But, anyway, that was their first chance to vent

1 and they certainly did and they still do.

2 Building the Blog, you're going to find an
3 internal champion that supports the Blog and in our
4 case it was very easy, we had our former
5 Administrator, Kip Hawley, he wanted the Blog and he -
6 - and so it started from the top and he basically,
7 this is before I came on board with the Blog, but he
8 basically made the threat that if you don't start a
9 blog, I'm going to blog on my own. So our Public
10 Affairs folks started wiping the sweat off their head
11 and said we better get a blog.

12 And so to build a blog you have to develop a
13 strategy, who do you want to be on your blog team?
14 Who do you - - how many posts do you want to put out a
15 week? Are you going to have a SOP, a comment policy?
16 And it all comes with assembly and a team. We worked
17 with the Communications Team, Legal was a huge help
18 and we wanted our Blog helping us with our Common
19 Policy and what we can say, what we can't say.

20 IT, and it's funny I mention IT because below
21 that Social Media can be cheap. Lynn Dean, who I'm
22 here for today, she was actually part of the team that

1 wrote out the Blog and the first time that - - after
2 Kip said he wanted the Blog, she went to somebody in
3 IT and said, okay, what's this going to cost us and
4 they gave her a figure of like \$650,000, just to start
5 it, and she was just flabbergasted and the next person
6 she went to said have you ever heard of Blogger.com,
7 it's free and that's what we use. So, of course, they
8 have to pay me, but I've agreed to live in my cubicle
9 and eat table scraps, so it's low budget.

10 (Laughter)

11 MR. BURNS: Pick the right people to do the work
12 and that's, Lynn actually found me, she knew about me
13 from, I was on the National Advisory Council, she knew
14 I was a subject matter expert on a lot of things that
15 go on in the field. I've been a field employee since
16 2002 and she knew that I had my own blog, so she
17 reached out to me and, of course, I jumped at the
18 opportunity to come up there, but somewhere in your
19 organizations, if you want to start a blog, you've
20 probably got the same kind of person out there that
21 has the right personality, the right experience to
22 have a blog and there's been times in the past where

1 CEO's have tried the blog and they're the subject
2 matter expert, they know everything about it, but they
3 try to blog and it just doesn't come off very well
4 because they don't have the right personality to deal
5 with it and they found a lot of times just to find
6 someone like me, that's just hanging in the field
7 somewhere doing their normal 9 to 5 might be, you
8 know, a better choice to get the message out.

9 Developing an SOP for your blog team is crucial,
10 you want everyone to be on the same page, you know,
11 here's what you can say, here's what you can't say, be
12 careful of SSI. If you're moderating you have to know
13 the Common Policy and the kind of comments that, you
14 know, can be published and the types that you have to
15 reject.

16 Building support internally, anybody you can find
17 that's an advocate of the Blog, involve them in some
18 way, ask them to write a post, or just add them to
19 your distribution list and talk to them now and then.
20 Everyone you have on your side is, the more the
21 better.

22 And raise awareness externally, that's been

1 pretty easy for us because still blogging in the
2 government is still kind of a new thing and kind of a
3 rarity, so people jump at the chance to write about
4 the government using Social Media on a regular basis,
5 but you want to go out and you want to spread your
6 link out, you want to spread your link out there, you
7 want to go out and make comments on other blogs and
8 build relationships with bloggers and get your link
9 out and share the message.

10 Just a few chief features of our Blog, we have
11 another way of humanizing the Blog. We have a meet
12 the Bloggers Section, where there's just a brief bio
13 on all of the Blog Team and it's a, you know, just a,
14 it's a little bit serious, you know, talking about our
15 background and then, you know, you add a little bit of
16 humor to it and, which, you know, once again, it kind
17 of humanizes us, we're not just, it doesn't sound like
18 a soloist robot spitting words at you, it's actually
19 somebody talking to you.

20 The Common Policy, we have it linked on the page
21 and it is, we'll get into the Common Policy later, but
22 it is linked and we often have to direct people to it

1 because they'll say why did you delete my comment and
2 it's all laid out there in black and white.

3 The delete-a-meter, what that is, is everyone
4 just automatically assumed that we were deleting
5 thousands of comments, that we weren't letting
6 anything through and that really surprised me, because
7 if you read our Blog, there's a lot of people that
8 really let us have it and we allow them to be
9 critical. Now if somebody comes on, or just says, you
10 know, you guys suck, I'm going to reject that, but we
11 do get a lot of that.

12 (Laughter)

13 MR. BURNS: And I don't take it personally,
14 because I know I'm not one of the guys they're talking
15 about. (Laughter)

16 MR. BURNS: But if they say, you suck and here's
17 why, we'll post that, as long as, you know, as long as
18 they're being somewhat respectful and there's a fine
19 line sometimes, but the delete-a-meter just, it shows
20 how many posts we've deleted since the beginning and
21 out of 20,000 comments that we've had so far, we've
22 only deleted, at the time this slide was made, a

1 little over 1,200 comments, which is a very small
2 percentage of deleted comments, and that includes
3 spam, that includes people who have posted five times,
4 because they didn't realize it was a moderated blog,
5 so they just keep on posting it. And then it includes
6 a lot of just really hateful egregious type stuff that
7 you would never want to read anyway, so if someone is
8 letting us have it, we let them have their forum.

9 Speaking of the Blog Comment Policy, the key part
10 in the beginning is TSA retains the discretion to
11 determine which comments it will post and which it
12 will not, so that gets kind of like the, you know,
13 everything all included there. We expect our
14 contributors to be respectful. We will not post
15 personal attacks. We won't post any personal
16 information, offensive terms, vulgar language, spam
17 and spam gets pretty tricky nowadays, people actually
18 go to the extent to hyperlink just a period and
19 they'll - - and you have to be really careful because
20 you never know what they're going to hyperlink to and
21 you - - it's easy to miss, unless you're looking for
22 it, but people do really try to get their Web pages

1 out there and, of course, we do not endorse, support,
2 or otherwise promote any private or commercial entity
3 and if you want to, this is all on the Internet on our
4 Blog page, which is TSA.gov/blog, you can take a look
5 at that and feel free to pull from it and use it, many
6 in the Government have and once again our Legal Team
7 was a huge help in putting that together for us.

8 Just a month after our launch, we received this
9 comment, "Wow, reading this Blog actually makes me
10 think that TSA might know what they're doing," and that
11 one was directed at me by the way.

12 (Laughter)

13 MR. BURNS: But we receive lots of great comments
14 and that's part of the great thing about working on a
15 Blog, because, 1) You never know what you're going to
16 be writing about. One day I'm writing about
17 formaldehyde, the next day I'm writing about camping
18 gear, you just never know what you're going to be
19 writing about, but you also never know what kind of
20 comments you're going to get and you get a lot of
21 funny ones.

22 A few I like to bring up every now and then was a

1 passenger said what are you going to do to address the
2 paranormal threat and they're like these ghosts can
3 walk past your checkpoints all day long and you'd
4 never know.

5 (Laughter)

6 MR. BURNS: And you got to kind of scratch your
7 head and think are they being serious, or you know.

8 (Laughter)

9 MR. BURNS: Or is this just a, or is this a joke.

10 And then you have people that are like, one of my
11 favorites, because it's just a visual, is, you know,
12 what am I going to do with my toothpaste, squirt it in
13 the pilot's eyes, you know, I get a kick out of that
14 one.

15 (Laughter)

16 MR. BURNS: And one of them said you thought my
17 banana was a bomb, it was actual a nutritious fruit.

18 (Laughter)

19 MR. BURNS: So we get lots of funny comments.

20 Now, Twitter, Twitter comes up a lot. We've been
21 using Twitter for over a year now and the reason I
22 signed up for a Twitter account for the Blog Team to

1 begin with was just to get the message out. Every
2 time that we had a Blog post we would go ahead and
3 just send a link out and say, hey, TSA has got a new
4 Blog post. We would also use it because Twitter, you
5 know, you can only have 140 characters or less and
6 Twitter is kind of a combination of a blog and an
7 instant messenger and I was also using it if we had,
8 like, just a quick update that we wanted to let
9 people, you know, let people know what's going on with
10 the Blog, but it really didn't warrant a new Blog
11 post, we would use Twitter to get that message out.

12 And what it's kind of evolved into is not only do
13 we get our link out there, but people are now starting
14 to ask questions on there and I do answer the
15 questions and I haven't really advertised that, for
16 obvious reasons, because of bandwidth, but now it's
17 starting to get more and more popular and we're
18 talking about putting together a team of Public
19 Affairs to actually address questions from the public
20 on Twitter, so they get, just a, you know, you're
21 getting ready to travel, oh, my God, can I take this
22 and you just tweet it and you find out.

1 But Twitter is also a great way, like I said, to
2 get a link out, it's kind of like throwing a rock in a
3 pond and watching all the ripples spread out the, it's
4 just you spread your link out just like that.

5 You have what's called re-tweets, I plot a Blog
6 post on traveling with diabetic supplies, the next
7 thing you know people are re-tweeting that to all
8 their diabetic communities and your link is just, you
9 know, I've got 3,000 followers, so 3,000 people have
10 my tweet, the other person has 3,000 followers, they
11 send it out and so on and so forth, the next thing you
12 know your link is just, poof, it's exploded.

13 But Twitter is a great way to expand on your blog
14 in getting the message out.

15 Here's some tips, and this was an actual Blog
16 post I put up, why did the chicken cross the road? It
17 was a Friday and I didn't really have much to Blog
18 about and I read a - - I read a thing in the news
19 about a chicken that was found on the side of the road
20 that was actually an improvised explosive device and
21 it had nothing to do with the TSA, but I just wanted
22 to have some fun, so I broke out all the chicken funds

1 I could find.

2 (Laughter)

3 Such as when they exploded the chicken it was
4 poultry in motion.

5 (Laughter)

6 Thank you, I'm proud of that one.

7 (Laughter)

8 But you have to have a sense of humor, that's
9 really important with the Blog, you want to - - you
10 want to get your message out, you want to be human,
11 you want to humanize your message and having a sense
12 of humor is a big part of that, I can't count, even
13 people that really hate the TSA have said, I got to
14 give you guys credit because you let us say what we
15 want to say, plus, you know, you're human, we, you
16 know, we can relate to you.

17 Establish a relationship with the readers. One
18 of them comes to mind and anyone from TSA Legal is
19 familiar with the name of Troll Killer and he's one of
20 our most popular bloggers, but he's actually the kind
21 of blogger I wouldn't mind seeing more of because
22 although he can be very critical of our procedures,

1 he's also our biggest fan and he'll actually stick up
2 for us in other forums and say, you know, I don't
3 agree with this, but TSA is actually listening to us
4 and they've done this, they've done that and it's
5 great to actually build relationships with those folks
6 and we actually have ended up sharing e-mails with
7 readers like that and they get more involved.

8 Those press releases is important, you see that a
9 lot in a blog versus kind of like another forum to
10 push out press releases and if people catch on to that
11 they're just going to go to your Web page, they don't
12 really need - - there really isn't a big difference
13 than what they're reading on the blog, other than they
14 can leave a comment.

15 When you make a mistake, right away if you've got
16 a mistake - - if you've made an error and you've put
17 something up that's inaccurate, you want to update
18 your blog post and make a public mention that, hey,
19 you know, we got this wrong, this is the right
20 information and you want to put like a little time and
21 date stamp, because if you don't there's people out
22 there that know if something's changed and they'll

1 claim you're trying to hide, to pull something over.

2 The Crew Guess Bloggers and the Agency, Chief
3 Council is posted on the TSA Blog before, some of our
4 more popular Blog posts, officers, anybody out there
5 is a subject matter expert. Of course having thick
6 skin helps.

7 And take the negative comments in stride. You
8 can really learn something from the negative comments,
9 that's one of the reasons that Kip wanted the Blog is
10 he wanted to see what people have to say and what we
11 were doing right and what we were doing wrong.

12 Now the internal social media, you heard about
13 the IdeaFactory earlier and as being a former field
14 employee, the IdeaFactory was a huge, just a huge
15 success because prior to the IdeaFactory, a lot of
16 officers in the field of all these different airports
17 had no way to communicate with each other. In fact,
18 you could have airports that were only like an hour
19 away from each other and it might as well have just
20 been, you know, on a different planet, people didn't
21 know if other airports were doing the same things they
22 were, if they had the same problems, if they wore the

1 same uniform, they really didn't know, but with the
2 IdeaFactory, it really opened up a lot of people to
3 communicate with each other, other officers and
4 managers out in the field and it enabled you to build
5 ideas, you know, for example, you know, why do we have
6 to wear these white shirts and the white shirts get
7 dirty, we were working the baggage areas, they're,
8 it's horrible and someone can build an idea on
9 anything and after they build the idea you can get
10 votes on it, it will - - it can build popularity and
11 it can actually, your idea, can be implemented, it's -
12 - would actually change policy and procedures based on
13 the IdeaFactory.

14 And as you can see from this clip, you can see
15 how many people have rated the idea, the average
16 rating, you can read comments, and this is also
17 moderated and we know who the poster is that actually
18 uses your government e-mail address, so it kind of,
19 it's a self policing site where you're really going to
20 have to do a whole lot to it.

21 But connecting the dots, by using the IdeaFactory
22 and the TSA Blog and Twitter and other uses of

1 social media we can figure out what the public and our
2 work force, what they're saying, what they want to
3 hear, what they want to see and kind of connect the
4 dots and make changes and try to win back the
5 passengers one at a time. Thank you.

6 (Applause)

7 MR. AMES: Hello, well, I think it's good to be
8 last, even though I guess I'm separating you and
9 lunch, but it's been actually nice to hear all the
10 other speakers go before and really address some of
11 the same issues that we struggle with.

12 So I'm going to talk about social media from my
13 perch in a program office. I'm in an Indoor Air
14 office with an EPA, specifically, working for the
15 Radon Program, so we're a small voluntary program and
16 EPA is doing a lot of great stuff with social media.
17 You may have seen Jeff Aleveor, head of Web
18 Communications speak at other conferences and they are
19 really doing many of these same things with blogging
20 and Twitter and really trying to get out there and
21 encourage program offices to take the plunge.

22 I really sort of stumbled into this. Our mission

1 is really to get information out to the public, to
2 prevent risks, so it really made sense for us to delve
3 into this area, but it's sort of good to know although
4 we approached this from a different perspective in a
5 smaller scale, we arrived at some of the same
6 solutions.

7 So this has been, I think, well covered today why
8 try social edia, there are a lot of good reasons, it
9 should always be related to your mission. For us it
10 really came down to public engagement, it's what we
11 do, public education, it's really the only tool in our
12 arsenal that we have, we don't regulate in our
13 program.

14 Also the idea of crowdsourcing, trying to be use
15 the ublic to get content and try to do things cheaper
16 and maybe better than you could do it yourself.

17 Another aspect is stakeholder engagement, which
18 for us is very critical because we really rely, in our
19 case, on our partners in the State programs and
20 industry to carry out a lot of the aspects of our
21 program, so we're always looking for ways to improve
22 communication and promote collaboration, so

1 interestingly the two things I will talk about today
2 are also things that Victor talked about, a contest
3 and building our own social network, I think just on a
4 smaller scale.

5 So the first thing the Radon Video Contest we
6 launched just about a year ago now and rather than
7 give you a background on the issue, I thought I would
8 just show you one of the entries and let it do my
9 talking for me.

10 (Video Playing)

11 (Applause)

12 MR. AMES: So that was not actually our winning
13 video, that was one of the Honorable Mentions, but I
14 never get sick of watching it. It really sets up the
15 issue nicely. This is something that EPA has now been
16 in the business, radon, for about 20 years and it's
17 always a tough issue and it probably always will be,
18 you know, it's odorless, it's invisible, there's no
19 bad guy, it's naturally occurring, so it's hard to get
20 that public outrage.

21 Let me just ask like how many people here have
22 actually tested for radon in their homes? Okay, not a

1 bad number, so if you don't remember anything else I
2 say today, please, please, go home, test your home,
3 I've done my duty today.

4 So one thing that we've done over the years to
5 get this tough message out is make use of public
6 service announcements, radio, television, print and we
7 still do this, we've had a lot of success over the
8 years, we've gotten millions of donated media time.
9 Really some of the first PSA's coming out of EPA were
10 in our program, where a lot, millions of people have
11 tested and fixed their homes as a result and it's
12 probably a strategy we'll continue to employ it well
13 into the future, but, you know, as years have gone on,
14 it hasn't gotten any cheaper and we've definitely
15 noticed diminishing returns, so quite simply, you
16 know, with traditional media we're up against a lot
17 more now. There are many channels, there are many
18 ways for people to really tune out, or skip past even
19 the best crafted message, TIVO, whatever it is.

20 So really thinking about online video was just a
21 way of trying to figure out where our audience is
22 going. And we really have a new generation of

1 home buyers we have to educate. We got a lot of free
2 media in the early to mid '90's when it was sort of
3 the new thing on the six o'clock News of what's going to
4 kill you in your home, but we have to keep that
5 message fresh, you know, and we have to look at new
6 ways and we need to be where our audience is, so that
7 was really what got me thinking at least about online
8 video and also it's just - - it's a good way to
9 interact with your audience, we will continue to use
10 traditional media, but most martyrs will tell you when
11 you have a passive, you know, radio or television
12 impression, you usually need to, you know, the Rule of
13 Seven, if you've heard this, takes about seven times
14 of viewing it before they're even going to process the
15 message. So although we may still get many more hits
16 from, you know, a place, a television spot, it's a
17 lot, I think, the impression that you leave with
18 online video is going to be greater, because people
19 had to search for that content, or they were e-mailed
20 it, or it was recommended another way, you know, they
21 have chosen in some way to view your message, so it
22 makes a little more sticky.

1 So these were all good reasons for me to propose
2 us getting online, YouTube, some of the other video
3 sharing sites, maybe repackaging some of our existing
4 material, or coming up with something new, the idea of
5 a contest really came out of, well, it's hard to say
6 what is going to work in, you know, that sort of
7 medium, so, you know, could we put our audience to
8 work and really ask them, you know, what is the most,
9 sort of compelling, or sticky message to get the word
10 out.

11 So I proposed a callous legal, technical and
12 budget issues, oh my, because I proposed that what I
13 thought was a simple idea, ask the public to create a
14 30 to 60 second public service announcements of their
15 own, there would be a theme, a test fix save a life
16 and as you saw from that introductory video, we asked
17 them to include our Web site and an 800 number.

18 Now, I didn't have, I wasn't thinking about all
19 these higher level things when I proposed this, I
20 thought this was something we could do as a program,
21 you know, I hadn't thought through all the
22 implications and so, you know, when I proposed this

1 probably back in about April of '07, surprisingly,
2 there was a lot of sort of concern about this and, at
3 that point, there was although there was lots of
4 private sector examples of a contest, there wasn't yet
5 any Federal Government example, I wish the State
6 Department had, a contest had occurred, at that point,
7 it may have made that a little easier for us, but one
8 thing we really needed to do was go to a lot of
9 different offices, the Office of General Counsel, our
10 contracts people and ask, you know, how, how can we
11 even do this.

12 One thing that we really wanted to do was offer a
13 monetary incentive. Now, this isn't necessarily
14 required when you're asking for user generated
15 content. Obviously, you've seen some good examples
16 of, you know, just having the idea out there and you
17 get a great response. Given that we didn't have sort
18 of a sexy issue, that was easy for people to wrap
19 their brains around, and we didn't really have a built
20 in constituency or network, to get the message out, we
21 really wanted some sort of a hook to draw people in,
22 so we talked to lawyers and dug down in the books and

1 what we actually found was this picture below. Does
2 everyone know what this is?

3 AUDIENCE PARTICIPANT: The Arlington Memorial
4 Bridge.

5 MR. AMES: Yeah, that's good, that's the
6 Arlington Memorial Bridge and as it turns out, in 1927
7 the Park Service ran a competition for the design of
8 the bridge, they offered a monetary prize and some
9 diligent auditor at the time said, isn't that a
10 misappropriation of government funds, so it went all
11 the way to the Comptroller of the Treasury, was a sort
12 of GIO of the day and said, no, it's okay so long as,
13 you know, government is really procuring a artistic
14 design, so that's what we were told, you can do this
15 so long as you're procuring artistic design, which
16 means you have to treat this like any competition, it
17 needs to be fair and open, we'd have clear guidelines
18 to score people against, so there's consistency and,
19 you know, you need to document it all the way through.
20 So we said, great, we'll run with that authority even
21 if it's, you know, 82-years-old, it works for us.

22 (Laughter)

1 MR. AMES: The settle on the prize amount, it's
2 not actually easy to cut someone a check in
3 government, so there's sort of a limit, so not
4 surprisingly my government cost estimate was
5 coincidentally the same amount.

6 So I'm not going to speak much about, I think
7 other people have done it better, the copyright
8 issues, you know, we thought since we are purchasing
9 something we did need to have people sign a waiver
10 which we adopted from some existing materials that EPA
11 uses for permission to use photos, we just added some
12 language, got the lawyers to sign off. Filing the
13 compliance was pretty easy since, you know, we only
14 picked one winner, we just had to caption that and we
15 were able to do that in-house.

16 So, essentially, we set up a registration site
17 where we laid out all those guidelines, you know, what
18 the theme was, background about the issues, who could
19 apply. One thing that I would really suggest,
20 whatever you're doing, any, whether it's a contest, a
21 blog, anything where you're having this
22 miscommunication, be as precise as possible, but

1 really avoid using legalize, because if you have fine
2 print that people aren't going to read, you're going
3 to end up with a lot of stuff that you can't use, or
4 you can't judge, so I think there are a lot of ways of
5 being very clear in what you're looking for without
6 getting in the jargon and at least our lawyers were
7 very supportive in, you know, that approach.

8 The issue of minors has been brought up. We did
9 have to add an extra step to identify minors, because
10 if a minor had won the contest, we would need a parent
11 or guardian actually to sign the, you know, copyright
12 and the other paperwork because you can't actually
13 have a binding legal agreement with a minor, so that
14 was an extra step, but fairly easy to do.

15 We decided to accept entries on YouTube and
16 encourage people to post it there. This was - - we
17 launched July of last year, so GSA had not yet signed
18 the YouTube agreement, so we had to be very careful
19 about this and we - - also a lot of people to send
20 entries directly to us and had a big disclaimer, but
21 it's much easier to do now, now that the government is
22 signing many of the special terms and conditions, this

1 is becoming a little easier, came up with some
2 evaluation criteria, creativity, quality, I thought
3 these were all very clever when I thought of them.
4 When I had to create a form to score everyone
5 consistently on them, it was a little more difficult,
6 but we did it and assembled a Technical Evaluation
7 Panel to look at this and really try to, you know,
8 keep good records and apply standard, as much as
9 possible, standard criteria in judging across all the
10 entries we received.

11 Marketing, I think, is the most important with
12 anything that you do in this realm. If you build it,
13 they won't necessarily come if they don't know it's
14 there. We really had a shoestring budget, which just
15 meant out own time. We used primarily social media to
16 market it. We targeted video makers, the sort of do-
17 gooder crowd, the environmentalists, and just a lot of
18 general social networks to get the word out, please
19 send this to your networks, you know, please let your
20 family and friends know about this.

21 Then we crossed our fingers, we gave people a six
22 month, or excuse me, six weeks to enter and with

1 anything I think you have to learn to be patient, you
2 know, after we did the marketing push and then there
3 was nothing for several weeks and, you know, I was
4 kind of nervous and going, okay, well this may be an
5 experiment that doesn't go anywhere, but don't
6 underestimate the power of procrastination, we ended
7 up with about 30 entries, which was about three more
8 times than I predicted to our management and many of
9 those came in the last 48 hours. They are all still
10 online and available to look at. They really range
11 from, you know, the good, the bad, the ugly, amazing,
12 I don't have time to show you any of the bad ones, but
13 I don't want you to walk away with the impression
14 that, you know, if you do something like this all the
15 content that's going to be generated is going to be
16 great, but I will say all the videos that are up
17 there, to date, have garnered about 21,000 views and
18 even the really bad ones continue to receive views and
19 even if it's just their family and friends that are
20 looking at it.

21 (Laughter)

22 MR. AMES: Hey, your message is getting out

1 there, you know, that is something that wouldn't have
2 been there before.

3 We got some newspaper and radio coverage and
4 we've now been the - - this, actually, the idea has
5 been replicated by our Water Office who got about 250
6 entries, so they really took the idea and ran with it.

7 And, finally, let me show you the winning video.

8 (Video Playing)

9 MR. AMES: So Eddie is a real person, he wasn't
10 the creator of the video, he was the star, but I
11 honestly don't believe that had we, you know, tried to
12 come up with the sort of best Web PSA ourselves that
13 we would have come close to something that as powerful
14 as just one person's true story. We've gotten, you
15 know, a lot of interests and a lot of hits on our
16 Web site and now actually several of the States have
17 asked us about pushing this as a television PSA since
18 it was actually one of the higher quality ones we
19 received, so, again, it was a little experiment and it
20 turned out to be a real winner as far as getting
21 usable content in getting our message out there.

22 So we shift now to the second area, and this is

1 the idea of promoting collaboration with stakeholders
2 and as I've already mentioned our primary stakeholders
3 are the States and industry that each are represented
4 by an organization that, you know, that we have
5 regular contact with. We have an annual meeting with
6 both groups and about, oh, two years ago we launched
7 this joint campaign and the idea was, you know, again,
8 let's double our results without any new resources,
9 just by improving the way we share ideas and
10 collaborate and share best practices. And we realized
11 soon, thereafter, that we had a lot of good tools, we
12 each had our own Web site at - - service, we didn't
13 really have one space where we could really
14 collaborate across those stovepipes.

15 So we sat down and agreed on some principles.
16 We'd, as three organizations, we make decisions by
17 consensus, we would build, we'd create the space based
18 on open dialogue and community self policing. Now I
19 think there are a lot of good reasons, especially with
20 the public, to allow for anonymous commenting, but we
21 really wanted to create a three-way conversation
22 between us and our members, not just, you know, us

1 communicating back and forth to them, but really
2 involve them, be involved in their decision-making and
3 us and theirs and theirs and ours, so we based a
4 principle, like everyone has to be named, register and
5 essentially, you know, state their affiliation up
6 front and we also built in some tools to allow the
7 community to police comments themselves and thus far
8 that's been a really workable strategy.

9 So let me just go ahead and show you, quickly,
10 what we came up with. More on this in a second, but
11 so here are the three logos of the organizations, we -
12 - the site is RadonLeaders.org which is not a .gov
13 site, so I'll talk about that just in a second, but,
14 again, the site has collaborative tools, a joint
15 calendar, an area for blogs, forums, you know, news,
16 really a resource area, really the only area that is
17 sort of top down, that isn't user generated, is this
18 front article where, you know, we as three
19 organizations try to push content usually about once a
20 month. So in creating this, we decided fairly early
21 on that we couldn't do this with EPA's Web
22 infrastructure and we wouldn't be able to probably get

1 the permission to do that, so the partner organization
2 The Conference of Radiation Control Program Directors
3 who represents the States is also our grantee, so they
4 agreed to run and operate the site, that which meant
5 that we needed to get special permission, again, going
6 back to the attorneys and say, well, how do we, you
7 know, co-brand this with EPA's logo, and what I didn't
8 show you on that page, was what we came up with, which
9 is a long disclaimer, but important so when people
10 arrive at the site, they understand that it's not a
11 Government Web site, that it's not necessarily the
12 opinions of EPA, that we are just one of three
13 organizations contributing and that's also really
14 informed the way we think about how as a staff we
15 approach this collaboration, we're very careful when
16 we go forward of saying, you know, this is, I'm
17 talking on behalf of myself, Jeremy Ames, as an
18 employee and/or here as, you know, our official policy
19 on this.

20 We also have to think about really the sort of
21 regulations that others have talked about, that were
22 put in place before the Internet, when we have this

1 sort of interaction. One of the things, if you look
2 at the article, we a couple of weeks ago solicited an
3 import for the development of a new long term strategy
4 for our program and we thought, well, what a great
5 venue to do this. Well, what - - many of the things
6 we had to think about when we did that was, you know,
7 Federal Advisory Community Act of regulations has to
8 be open to everyone. Anyone can register for the
9 site, it's obviously targeted at a certain group, but
10 we can't restrict who we ask information from if
11 they're giving us input, Paperwork Reduction Act, you
12 can't ask, you know, a standard set of, you know,
13 multiple choice questions without triggering this
14 whole other requirement, so we're conscious of that,
15 but we really are, I think, able to have these sort of
16 interactions and, you know, to date we've had about
17 470 registered users, which considering the whole
18 community, is maybe a couple thousand, that's been
19 pretty amazing, about 200 or so user generated
20 contributions, which is very good, but I, of course,
21 look at that number and go, well, that means over half
22 of our users have yet to make their first posts and

1 that is always the chicken or the egg with user
2 generated data, you really need to seed it, so people
3 are looking at it, interacting, commenting and have a
4 reason to come back and until the ball gets rolling
5 that's always a challenge, so we worked very hard at
6 really keeping, putting up new content and adding
7 features as people have requested, like the blog
8 feature, for example, is not something we originally
9 included, we thought people could be blogging
10 elsewhere, they probably already are, there is a
11 demand for it and it's proving to be one of the more
12 popular features.

13 So, again, I think there are a lot of benefits to
14 using social media, you just really have to look at
15 how it relates to your mission and then find the
16 people within your organization, maybe many of the
17 people in this room who you need to work through, work
18 with, to work through some of the issues, because I
19 think that if there's a will, there is a way and the
20 more that we try to do this as a group here, I think
21 it makes it easier for others to come in and innovate
22 and get involved in the process, so.

1 (Applause)

2 MODERATOR SAND: We have a couple minutes for
3 questions, if anybody wants to line up in front of the
4 mike.

5 And while we wait, I just want to thank our
6 panelists again for doing such a great job in helping
7 orient us to this technology and what it's like to
8 actually manage it and create it, so thank you to the
9 panelists.

10 (Applause)

11 MODERATOR SAND: Can we have our first question?

12 AUDIENCE PARTICIPANT: Yes. As a member of the
13 longest running, most hated Agency in the Government,
14 the IRS - -

15 (Laughter)

16 AUDIENCE PARTICIPANT: But I'd like to ask, do
17 you, other than the occasional e-mails you get, do you
18 have any other facts that you can back up, or
19 something more demonstrable of how a blog is - - helps
20 humanize your employees at something we've been
21 looking at, humanizing the tax collectors?

22 (Laughter)

1 MR. BURNS: So your question was blog posts that
2 humanize, like for example, is that what your question
3 is?

4 AUDIENCE PARTICIPANT: Have you seen any - - what
5 - - your comment was that you felt a blog helped
6 humanize the, how - - what are you basing that on
7 basically, or how many comments you get back in the
8 blog?

9 MR. BURNS: Right, I base that on - - so many
10 times you read government press releases, or go to a
11 government Web page and what you're reading is very
12 bland and lacks personality, it's just kind of like,
13 here's the facts and laid out in a very professional
14 way, where they almost lead you to believe that you're
15 being talked to by a robot.

16 Where we're totally opposite of that, when we
17 communicate on the Blog we just try to chat as we were
18 just chatting, you know, at dinner or over coffee, we
19 try to, that's the way we, you know, humanize our
20 message and show that, hey, we are real people, I do
21 have hobbies, interests, the same as you do, I'm not
22 just a 9 to 5'er, working for the Government and the

1 Government's my life and that's all I care about and
2 so does that answer your question?

3 AUDIENCE PARTICIPANT: Yes.

4 MR. BURNS: Okay.

5 AUDIENCE PARTICIPANT: I'm back. This time, I
6 wanted to say that I think it's brilliant to engage
7 the public because some of your best ideas are going
8 to come from somebody outside the organization and
9 that's really smart, but I also wanted to ask because
10 you mentioned building a blog and starting something
11 like this for your organization and who to go to and
12 how to go about it and there are a couple of things I
13 saw missing and I wanted to find out for sure if
14 you're doing that or not.

15 First, of course, is the OPSEC people, you want
16 to talk to them, and the other is your IT people,
17 because besides OPSEC, I'm also an IT guy and I think
18 a lot of people underestimate how much information you
19 give away if you're not paying attention, things like
20 the metadata and errors and messages on your Web
21 server and how that facilitates attack and then
22 perhaps defacing of your Web site, and that sort of

1 thing, and I'm wondering if you're handling that in
2 any way, if you're looking at that, and, if so, how
3 are you handling it?

4 MR. BURNS: (Sound of a bird tweeting).

5 AUDIENCE PARTICIPANT: And nothing okay.

6 MR. BURNS: As far as I'm concerned, that's
7 really out of my area of expertise, but I do know that
8 we are -- IT Department and Legal are heavily involved in
9 those decisions, but, I mean, personally, I'm just a
10 blogger.

11 (Laughter)

12 AUDIENCE PARTICIPANT: Yeah.

13 MR. BURNS: But, I don't know, or if Jeremy has a
14 better answer.

15 MR. RICHE: I, actually, at the Department of
16 State we have industrial strength firewall and other
17 software to go ahead and to stop those kinds of things
18 and it's definitely part of the consideration of
19 operating, plus some of our public Web sites are
20 totally off our system, they run by the private
21 sector, so there is no connection there.

22 MODERATOR SAND: And just a reminder, there's a

1 whole Security Panel at the end of the day, you can
2 ask the questions later.

3 AUDIENCE PARTICIPANT: Well, this has less to do
4 with traditional security than OPSEC, because an error
5 message isn't something a firewall is going to stop,
6 that has to be done in the code and on your Web server
7 settings, so - -

8 MR. AMES: Yeah, that's handled by the commercial
9 provider that handles - -

10 AUDIENCE PARTICIPANT: Well, yeah.

11 MR. AMES: Right.

12 AUDIENCE PARTICIPANT: Okay, all right, thank
13 you.

14 MR. AMES: I would just add, anything that we do
15 on our Web site, you know, goes through that process.
16 The stuff we've done off, we use - - we decided to use
17 Drupal, which is an open source platform and really
18 it's sort of the same way as we approach content
19 development, you know, we ask some people to basically
20 try to crash it, you know, test it out, different
21 browsers and, you know, just try to be quick at
22 responding because as much as you try, there's going

1 to be something that doesn't quite go right for some,
2 but a portion of your user base and so I've just got
3 someone, a contractor we work with, who is very
4 quickly able to sort of respond to that, but it is a
5 little different than - - and I think gives us a
6 little more flexibility than what we would be able to
7 do on our own site.

8 AUDIENCE PARTICIPANT: Thank you.

9 MODERATOR SAND: All right, well thank you very
10 much for being with us for this first Panel.

11 (Applause)

12 It is now lunch until 1:30; we'll meet back here
13 in this room for the rest of the Workshop, thank you
14 again.

15

16 (Luncheon recess 12:00 - 1:30)

17

18 Panel 2: How does Government 2.0 impact privacy?

19 Moderator Landesberg: We will come to order now.

20 I'm Martha Landesberg, Associate Director in the
21 Privacy Office for Privacy Policy and Education.

22 Thank you all for being back here so promptly.

1 We have a really interesting and detailed agenda
2 for you over this day and a half and I just want to
3 say how much I appreciate the presentations we've
4 heard this morning.

5 We've heard a lot of really creative and
6 interesting voices of social media. Some of which is
7 personally identifiable information from users and
8 some do not. We heard a lot about building teams
9 together to identify and address issues as they come
10 up in the use of this new media.

11 Really, the rest of our workshop is going to
12 begin now with a series of panels on the issues and
13 uses of social media by the Government and ways.

14 This panel is about what issues are raised when
15 the Government chooses to use personally identified
16 information or to collect it when it uses social
17 media.

18 I'm very happy to introduce our panelists to you
19 and tell you a little bit about how they're going to
20 use this next hour or so.

21 Our panelists are Jonathan Cantor, who is the
22 Executive Director for Privacy and Disclosure at the

1 Social Security Administration.

2 Danielle Citron, a newly minted Professor of
3 Law at the University of Maryland. We want to
4 congratulate you on that.

5 We're looking forward to having Lillie Coney, who
6 is the Associated Director for EPIC, the Electronic
7 Privacy Information Center; who will join us
8 momentarily.

9 Tim Jones, who is Activism and Technology Manager
10 for the Electronic Frontier Foundation.

11 Jay Stanley, who is the American Civil Liberties
12 Union's Education Director in the Technology and
13 Liberty Program at ACLU; and Heather West, who is a
14 Policy Analyst for the Center for Democracy and
15 Technology.

16 We are going to go through a series of questions
17 -- there you are. Hey, Lillie, welcome.

18 With everyone here, let me just say again, we're
19 going to cover a series of questions. I'll be posing
20 a question to each of my colleagues on the panel to
21 try to get at the question of how and whether
22 Government's use of social media can impact on

1 individual privacy.

2 Each of the panelists will provide an answer to
3 that question and they will begin to pose questions to
4 one another, and we hope that in this hour and 15
5 minutes or so we will begin to give you all a flavor
6 of the issues, as these experts have been thinking on
7 this for quite a while, and can elucidate for us
8 today.

9 So I would like to start and then sit down and
10 let them really talk to each other.

11 I'll ask you Danielle, just to give you all a
12 little bit of a background on what we're beginning to
13 learn about what individuals' expectations are when
14 they interact with the Government through social
15 media.

16 So, Danielle, what do we know so far about
17 individuals' understanding of Government's role in
18 social media and do they have particular
19 expectations about how the Government uses their
20 personal information in this context?

21 Ms. Citron: It might be too early to tell in any
22 really clear way of what our expectations are, at

1 least in a studied manner. I think some of the
2 signals that the Obama Administration is giving us
3 will give us a sense of what the public is actually
4 expecting, when it comes to interactions with social
5 media, when they join Facebook groups or sponsored by
6 the EPA or friend the President on MySpace.

7 We know that, of course, the January 21st memo,
8 the Open Government Memo, talks about the importance
9 of using these social networking tools or using
10 technologies to enhance Government's transparency and
11 the public's participation, and to collaborate with
12 the public on policy matters.

13 A while back a White House spokesperson had said
14 the goal is to have increased what we know about
15 Government, but really not the other way around.

16 So, you know, what does that mean for our
17 expectations for our privacy when we interact with
18 Government on social networking sites? I think that
19 it really creates an assumption of openness when it
20 comes to our interactions with Government on policy-
21 related matters. These two-way conversations we have
22 with Government, common sections, and a presumption of

1 privacy, when it comes to information that relates to
2 our private information.

3 So, for example, what we write on the wall, the
4 25 things that you don't know about me. I think there
5 is a presumption of privacy in that personal
6 information. I think the metaphor of a one-way mirror
7 is very helpful here. That is, we want people to peer
8 into Government's workings and to have transparency
9 for those two-way conversations about policy or three-
10 way conversations about policy; but at the same time,
11 that Government or agencies shouldn't be able to peer
12 back on the other side of the mirror, peer into
13 individuals personal lives and information, even
14 though they funded the President so-to-speak, and let
15 their friends peer in. I think that Facebook's sort of
16 model in architecture here, that having found pages
17 for agencies, is really instructive and supports the
18 intuition.

19 Facebook allows or creates -- agencies have
20 Facebook pages where they have fans, so that
21 individuals can comment on policies, can see what an
22 agency is talking about, and what it's doing. But at

1 the same time, the agency can't see what its fans
2 personal story is. You know, what they write on their
3 walls. I think that position is really normatively
4 appealing, because if the whole point of the open-
5 Government directive is to enhance our participation,
6 knowing that the Government isn't peering inside what
7 we're doing inside personally, it's really going to
8 enhance our willingness to friend the President or
9 friend an agency or join a Facebook sponsored group.

10 Moderator Landesberg: Thanks Danielle.

11 Does anyone else on the panel care to comment on
12 this topic?

13 Okay, Lillie, let me ask you. What Government
14 uses of social media, pose a privacy risk to
15 individuals or could, and what precisely are the
16 privacy harms that could result?

17 Ms. Coney: Well, the contact of social
18 networking, it's a new form of communication that
19 people are recently beginning to use. It's the
20 Federal Government's latest arrival to the process,
21 which involves the collection and use and sharing of
22 very personal, sometimes identified more information,

1 and it's a lack of regulations of rules about what the
2 role Government should play in its involvement.

3 Now, all agencies aren't the same. They don't do
4 the same types of things. Some provide benefits.
5 Some provide services. Some provide information.
6 Some are regulatory. Some are law enforcement. Some
7 are defense in nature. So, the way they might want to
8 engage or use the technology will be very different.
9 So, for instance, if we look at how the Government
10 will engage in this new medium, is it going to
11 consider itself to be a friend? Is it going to be
12 like a corporation that has a Facebook page or
13 identify space online, or will it be something
14 completely different? Will it be a super user in some
15 respects, where the boundary between what people's
16 expectation is regarding friending of a Federal
17 Government agency or friending a corporate identify
18 online or even friending another individual is
19 completely different. So, how the information will be
20 used, who it might be shared with, what purposes it
21 might be put to, all of those questions have to be
22 answered by Government setting a foundation for

1 transparency, openness, and respecting privacy rights
2 of users while online.

3 It may be that it is very easy to look at issues
4 about pushing information out, providing information
5 to individuals. Some of the things that we have
6 seen over the last few weeks, H1N1 or even now that
7 we're entering hurricane season, there is a good
8 reason why Government may need to speak to individuals
9 regarding certain circumstances, but then when we get
10 beyond that, when you talk about the potential for
11 collecting and using information, the privacy rights
12 of individuals could be greatly diminished, and it
13 could be enhanced, depending on what the rules are --

14 Audience: We can't hear you back here.

15 Ms. Coney: Oh, I'm sorry.

16 The privacy rights of individuals can be either
17 diminished or enhanced depending on how Government
18 actually uses social networking services. Work on
19 issues like, Government profiles, identify theft,
20 which is a growing problem and has been for several
21 years.

22 Now with the advent of medical identify theft it

1 even becomes more important to protect information.
2 What about loss of job opportunities, loss of
3 employment? There are some services that are coming
4 online where the Government wants to be able to do
5 employment clarification. What about it being used as
6 a motivation or as a part of an investigation of
7 varying types; loss of promotion benefits could make
8 people more vulnerable to attacks that have a legitimate
9 concern about who has access to information about
10 themselves. Not just to mention women or those who
11 have been victims of violence; domestic problems,
12 stalking, sexual assault, but also people who have
13 been a victim of other type of physical threat of harm
14 posed by others.

15 Also, the effect on free speech, because
16 it may not just be a matter of what the Government is
17 actually doing, it's also what people's perceptions of
18 what the Government is doing. So, transparency
19 becomes very, very important with how the Government
20 engages online.

21 Moderator Landesberg: Tim, do you care to chime
22 in on that question?

1 Mr. Jones: It's tricky. The thing that I'm sort
2 of most interested in is in talking about some of the
3 ways that the third-party interactions with Government
4 Web sites can affect privacy. I think, increasingly, I
5 don't think its news to anyone here that a Web site is
6 not really a single-source document at this point.
7 Sort of part of Web 2.0 has been, that if I go to a
8 Web site, I'm actually -- a lot of the services and
9 data that I'm seeing, may be coming from a variety of
10 different places. Every Web 2.0 company and every
11 aspect of it has a way of leaking. You can embed this
12 in your site. You can put a badge in your site. All
13 of that is hosted on their servers, on servers that
14 aren't owned or controlled by the Government agency.
15 This can present some real privacy risks that I think,
16 it certainly -- Danielle was talking earlier about
17 expectations of privacy on social networking sites.
18 The reason that it is complicated is because, I think,
19 when you have a traditional interaction with the
20 Government, whether it's IRS or CDC or Congressional
21 Representative or the White House, there is a
22 presumption of privacy from other people in there that

1 you're not going to have corporations looking over
2 your shoulder and taking notes, while you're trying to
3 get information that is going to help you make
4 decisions about your health or your life or anything.

5 I'll use the Whitehouse.gov as an example. I
6 want to caveat that I'm a huge fan of the White House
7 Web site. They've really done some great work and I
8 don't want -- I know that a lot of it was launched
9 pretty remarkably quickly and so I really want this to
10 be taken in the spirit of constructive criticism,
11 especially since the White House is leading the pack on
12 a lot of this Government 2.0 efforts, and the site is
13 in a lot of ways being used as a blueprint for future
14 efforts.

15 If I go to Whitehouse.gov there are a number of
16 other entities in serving content there. Probably the
17 most significant data-wise is YouTube, which they're
18 now using to embed videos on the Government Web site.
19 There was a problem when they first launched and it
20 has to do with that Government-cookie policy, which I
21 don't think anyone likes. As tricky as it is when
22 you're building a normal Web site, it's even harder

1 when you've got third-party cookies involved. I think
2 when Whitehouse.gov re-launched with YouTube, embeds
3 that were persistent cookies from YouTube being put on
4 people's Web browsers, that was allowing Google to log
5 information. Initially, about every single person
6 that visited Whitehouse.gov, if you had logged into
7 YouTube with your personal account, which is now
8 connected to your Google mobile, which is increasingly
9 going to include information on every aspect of your
10 life, they're now connecting information -- they were
11 for a short time collecting information about
12 potentially everything you do on Whitehouse.gov there.

13 There was a really fast change made by both the
14 White House and YouTube and Google, where they rolled
15 out a new feature, very quickly, called Delayed
16 Cookies, which is such a silly name given for the
17 important concept.

18 It was based on a project that we worked on at
19 the Electronic Frontier Foundation called MyTube,
20 which means that they can't place cookies on a
21 visitor's computer until you actually click play on
22 the videos. So, it was a great step and it was done

1 amazingly quickly, but it still means that if you go
2 to Whitehouse.gov and you play a video, YouTube is
3 able to log that you, and does log, that you have
4 viewed that video in association with your YouTube
5 account. That's just because it's the default
6 behavior for YouTube.

7 When you view an embedded video in anybody's
8 Web site, the YouTube cookies are used to keep a log of
9 every video your account has viewed.

10 So, there have been a few changes since then.
11 EFF wrote some letters to the White House General
12 Counsel about it. There are some articles on CNet;
13 the privacy policy was updated a little bit, but there
14 are still some problems with it. There is some real
15 daylight between the White House's privacy policy and
16 YouTube's privacy policy on this and it has not --
17 exactly, what's going on here hasn't been clarified by
18 either group.

19 The White House privacy policy says these
20 persistent cookies are used by some third-party
21 providers to help maintain the integrity of video
22 statistics. A waiver has been issued by the

1 White House Counsel's Office.

2 If you look at YouTube's privacy policy and how
3 it uses cookies, it says, oh, we use cookies to do an
4 analysis of five different things, a lot of which go
5 well beyond video statistics. It has things like we
6 use them to provide custom personalized content in the
7 information or to monitor the effectiveness of our
8 marketing campaigns. So, now you've got your personal
9 interactions with the White House or indeed with any
10 Government Web site that uses embedded video being used
11 to help Google's marketing campaigns, which is harm
12 and is inappropriate.

13 Here at the Electronic Frontier Foundation, we
14 have been trying to talk with YouTube about it. We've
15 received a sort of back channel confirmation that, oh,
16 right, we're going to stop blogging this, but only for
17 Whitehouse.gov, but it hasn't been publicly or clearly
18 described by YouTube as to what's happening.

19 The result is really ambiguity. The media
20 coverage of that change was; you can't find anything
21 about it on YouTube's Web site or the White House's
22 Web site. Where things stand, I think it is pretty

1 difficult for both privacy and for innovation and on
2 some Government Web sites like Congressional Web sites,
3 YouTube videos are being embedded even without delayed
4 cookies and so the privacy problems persist on a lot
5 of Government agency Web sites, which I'm sure a lot of
6 people here know, you almost never find YouTube
7 embedments. I imagine a lot of that is because of the
8 confusion around YouTube embeds, in fact, with cookie
9 policy. So, if CDT have put out some recommendations
10 for changes to that policy that would, I think, help
11 both privacy and progress and innovation in Government
12 Web sites.

13 That's just an example of that kind of problem
14 that you can have as you start to integrate these
15 third-party services into new Web sites.

16 Moderator Landesberg: Thanks Tim.

17 Let me just follow up with a quick question and
18 anyone else could join in as well.

19 Do you see the privacy impact, the potential
20 impacts, any differently if we're talking about the
21 use of third-party technology on a Government site or
22 the Government's placement of content on a third-party

1 site? Are differences there?

2 Mr. Jones: I think the common thread, and anyone
3 else can join in, is that the expectations need to be
4 clear. Right now there is real ambiguity around this
5 issue with YouTube. You're seeing different things
6 from the White House's Web site and YouTube's Web site or
7 if you look on EFF's Web site, you've gotten certain
8 theoretical concessions from them, but it's vaguely
9 described in our blogs, the blog post on Web site and
10 most people visiting those Web sites don't know
11 anything about it.

12 I think whether you're on Facebook or
13 Whitehouse.gov or any agency Web site; yeah, I wouldn't
14 be able to speak for legal questions, I'm not a
15 lawyer. So, I'm not certain how the Privacy Act and
16 all that applies in these cases, but just from a
17 consumer advocacy standpoint, you need to make really
18 clear to people what's going to happen to their data.
19 Both when it's used by third-parties and when it's
20 used by the Government itself.

21 Ms. Coney: This has been an issue where
22 Government using contractors or third-parties to

1 manage information or provide services that implicate
2 personal identifiable information. There's a problem
3 that when you are not talking about a Federal
4 Government agency managing, collecting and using that
5 information then the Privacy Act, even the Freedom of
6 Information Act, it doesn't apply. So, unless there
7 is a contractual understanding, an agreement between
8 the Government agency and that third-party that it
9 will apply, then you are digging us deeper into this
10 hole where data is going and there is no ability to
11 really create transparency that's reliable for the
12 consumer as well as for oversight agency or those who
13 would be concerned about how this information is being
14 used.

15 Moderator Landesberg: Thanks Lillie.

16 Danielle, did you want to say something?

17 Ms. Citron: I think that there shouldn't be any
18 difference because if what we want is to enhance more
19 participation to garner the expertise of the public
20 then the guarantees and concerns about not wanting --
21 really underscoring, not wanting to show involvement
22 because we're worried about being tracked or spied on.

1 I think we ought to make sure that we have parity
2 amongst the sites so that we can encourage more people
3 to participate.

4 Moderator Landesberg: Anyone else on that point?

5 Let's turn for a moment now to Jay.

6 Are there social media activities in which the
7 Government should not engage and should there be any
8 limits on the Government's use of personal information that
9 any individuals submit on social media?

10 Mr. Stanley: Yes, I have a list right here.

11 Moderator Landesberg: Okay.

12 Mr. Stanley: No, I wouldn't make a blanket
13 statement like that, I don't think. I think that -- a
14 couple of things, a couple of points.

15 Number One, we're in an era where there is a
16 large infrastructure for the collection of information
17 about individuals on the part of the private sector on
18 the Internet for purposes of tracking and advertising.
19 In some ways what we're seeing here and what Tim's
20 talking about is the Government moving into a
21 collision with that large infrastructure in ways that
22 are often incompatible.

1 Also, I mean, when we're talking about social
2 networks, what's a network? A network is a set of
3 nodes all of which are presumed to be equal. It's not
4 a hierarchy where one is the top and everything else
5 is below. So, when you talk about Barack Obama
6 joining your network and when you friend Barack Obama,
7 are you friending him or are you friending the entire
8 executive branch? There is a huge power difference
9 here, okay? This is not like your three friends and
10 Barack Obama, unless you went to law school with him
11 or something. So, I think that in some ways, the
12 social network is not the right technology for
13 citizens to interact with Government because it's
14 premised on equality in a way that just doesn't exist
15 in individual's relationship with their Government.
16 It's kind of like the Lochner Era of Jurisprudence,
17 you know, the turn of the century -- first couple
18 decades of the century where the courts were saying
19 like well, you know, you can't regulate wages and
20 hours, because it's just you, Joe Schmo and General
21 Motors and the two of you as equals are reaching a
22 deal. That was obviously a fiction.

1 In some ways, you know, the idea that you can be
2 a part of an equal social network with your Government
3 is a fiction, too. So, I think the agencies need to
4 be aware of that.

5 What was the second part of your question again?

6 Moderator Landesberg: Well, just asking whether
7 there ought to be, in your view, there should be
8 limits on how the Government uses personal information
9 that it does collect through social media?

10 Mr. Stanley: Yes. I mean, I fully agree with
11 Danielle's excellent point about the one-way mirror.
12 I think that unless there is a very good reason or
13 purpose or goal that it should all be a one-way
14 information flow. Of course, there are probably very
15 good, cool ways that Government could engage with
16 citizens that which might involve gathering
17 information from them.

18 You know, this morning I was looking forward to
19 hearing more detail, than I was aware of, of how
20 Government was using social network. I was interested
21 this morning and most of what we heard about was sort
22 of a one-way push of information out.

1 I think it's great that the Defense Department is
2 using 18 different, you know, cool social networking
3 systems to pump information out about there.
4 Although, I am always thinking to myself that
5 transparency is good, transparency is good, but if it
6 just means like information that is, basically,
7 already available is sort of advertised better. I
8 mean, that's great, but the real problem of
9 transparency is the out of control secrecy system that
10 we have in our Government and that isn't addressed at
11 all by switching over to you know -- I would rather
12 have the Defense Department reveal everything that
13 they should reveal and not hide things because they're
14 afraid of being embarrassed, and put it all on a flat
15 Web site then have their own selected information that
16 they chose to reveal, and have it pumped out by 18-
17 trendy social networking systems or something.

18 Obviously, there do need to be rules in place.
19 There needs to be purpose, verification, use limitation,
20 and data minimization. These are very well established
21 privacy principles in the privacy world.

22 When you collect information, you express what

1 the purpose of collecting that information is, and you
2 don't use it for other purposes without the express
3 permission of the subject. You only collect as much
4 as you need for the purpose at hand and so forth.
5 These are very well established privacy principles.
6 So, if I were in the Government looking at building
7 these kinds of applications, the first thing you would
8 do is familiarize myself with all of these very well
9 established principles and figure out how I was going
10 to apply them.

11 Moderator Landesberg: Thanks Jay.

12 Heather, let's talk for a little bit about your
13 views on what the privacy framework ought to be for
14 Government use of social media.

15 Ms. West: Well, I think to start looking at what
16 the privacy framework should be we can look at the
17 history of privacy as the Government collects
18 information and uses information about people.

19 I think everyone has already mentioned that this
20 should be a one-way mirror. That they should minimize
21 the amount of information that they are taking off of
22 a social media site and talk about, maybe, it should

1 be a one-way push, and how do we use the
2 interactivity, because that interactivity involves
3 personal information on a social media site, more or
4 less by design.

5 So, right now, the main law controlling how the
6 Government collects, uses and interacts with citizens
7 and their data is the Privacy Act from 1974. It
8 hasn't been substantially updated since then, despite
9 all of the advances in technology; they certainly
10 weren't thinking about social networks and MySpace or
11 YouTube when they wrote the Privacy Act. So, it's
12 definitely not allowed for -- it doesn't allow for
13 information the Government hasn't been specifically asked
14 for and doesn't specifically need.

15 So when I friend Barack Obama on MySpace, he has
16 access to everything that the rest of my friends have.

17 You mentioned the power imbalance there. So, the
18 Privacy Act tries to -- is based on a set of fair
19 information practices from the 1970's. There are
20 several iterations, but they all involve telling
21 citizens what information you are collecting. Telling
22 citizens what uses that information is being put to

1 and giving them some sort of recourse to say, I think
2 your information about me is wrong. So, that basis on
3 the Privacy Act has provided 35 years of pretty good
4 privacy policy. Unfortunately, because of the letter
5 of the law of the Privacy Act, it doesn't cover
6 anything that the agency doesn't control, as you
7 mentioned. So, because the information on MySpace or
8 Facebook or YouTube is not under the agency's control,
9 even if they have access to the information, which
10 they may not in the case of those third-party Web 2.0
11 technologies, it's not covered by the Privacy Act.

12 We're working on some updates to address this kind
13 of technology and trying to address -- you know,
14 information should be covered by the Privacy Act,
15 whether or not it's controlled by the agency, if the
16 agency is using it. But all of this calls into why
17 agencies need to have their own policies about this
18 stuff. They need to think about it proactively before
19 they go to Facebook and MySpace.

20 Moderator Landesberg: Thanks.

21 Are notice and choice sufficient in this area?

22 Anyone on the panel want to address this?

1 Ms. Coney: Yes.

2 Moderator Landesberg: Go ahead Lillie, please.

3 Ms. Coney: Notice and choice present some
4 interesting problems because we see notice all the
5 time. It's a strict shrink-wrap licensing. You're
6 about to download some software, the screen pops-up,
7 this is the agreement, the terms and conditions for you
8 to purchase. How many people read that thing? I
9 mean, you want that software and you want that update,
10 you want whatever you want, right then and there.

11 You click okay and you download the software and
12 just hope it's not actually an agreement to take over
13 your computer. That's pretty much how notice and
14 choice is working out there in the commercial sector.

15 It's important for people to have that balance.
16 When we're talking about the Government as a friend,
17 it's not an equal -- I mean, Jay is absolutely right.
18 The other panelists, Danielle, and they've all pointed
19 to this. It's very difficult to treat the Government
20 like it is an individual. I think that's --
21 Government agencies understand they have authority to
22 do things like put people on "No Fly List" or to

1 decide whether someone qualifies for a benefit or
2 service, but we cannot go into this treating
3 Government agencies as if they are equivalent to
4 individuals.

5 When the only thing that somebody who has
6 friended you might be able to do is to decide to
7 unfriend you or blog about something you may have said
8 that they didn't like.

9 I think it's very important to also remember the
10 history of Government agencies and communication
11 service providers. That it has a long track record of
12 agencies who have a need for information or desire
13 greater access to communications, going around to the
14 service provider, whether its wire communication like
15 Western Union's and so forth or the Shamrock Program
16 that ran for several decades to programs like
17 COINTELPRO, where people were targeted because they
18 were engaged in Civil Rights or anti-war activities in
19 the 60's, and in the last decade. But literally,
20 people who were exercising constitutionally protected
21 speech were being targeted and their telecommunication
22 may have been tapped or even in the last decade where

1 FISA, which was in place and intended to provide a
2 legal pathway to get access to telecommunication, was
3 bypassed completely.

4 So, assuming, that if we don't do anything or say
5 anything it won't be a problem, I say history says
6 otherwise. So, it's important for us to have the
7 right approach to transparency that Jay talked about.

8 EPIC proposed through some recommendations to
9 Whitehouse.gov, but fundamentally don't check users
10 while they're participating in online Government
11 social networking opportunities; just don't do it,
12 don't collect the data. Direct those who have
13 contracts with these agencies that they cannot collect
14 the data and then make sure that the system is
15 designed not to collect the data.

16 I think we have to start approaching the process
17 by establishing what the rules are and then design the
18 technology to accomplish those particular goals.

19 Moderator Landesberg: Great; thank you Lillie.

20 Danielle, do you want to chime in?

21 Ms. Citron: Just one thing about notice and
22 online social networking sites.

1 It's an interesting study from 2008, published by
2 ACM about how individuals, when they sign up for
3 social networking sites, they typically default to the
4 settings -- privacy settings, I think, like, 87
5 percent of leasing MySpace users, default to the
6 privacy settings that are preferred by, let's say
7 MySpace, and it's the least privacy protected of the
8 choices of the menu. So, I think it's worth putting
9 in our hopper how we think about notice and whether we
10 exercise our privacy protections just as a matter of
11 human nature.

12 Mr. Stanley: I think that overall, I mean notice
13 -- we all understand that our money is limited, but
14 our attention is also limited, and we are flooded with
15 information with click-wrap contracts and so forth,
16 and it really is pushing contract law to a reductio ad
17 absurdum very quickly.

18 Basically, when you agree to one of these
19 contracts, that's got blocks and blocks of print,
20 you're basically trusting that the laws are basically
21 sound enough, like nothing too outrageous could be in
22 there. You're not signing away your first-born child

1 or anything. You're basically forced to trust. Like,
2 the general legal structure of our society is such
3 that nothing to crazy could be in there. In some
4 cases that legal structure is not good enough and so
5 we need to strengthen it as Lillie was saying.

6 Moderator Landesberg: Thanks.

7 Heather, did you want to add something?

8 Ms. West: I did. I think an important point was
9 brought up around the terms of service. The
10 Government has the opportunity here to really
11 negotiate privacy protective terms of service, because
12 they're not a person. They are an agency.

13 The GSA has a great deal of influence in saying
14 here's what we need you to do with your data that you
15 collect from our site before we're willing to give
16 you this traffic, and that can really end up
17 influencing the marketplace of privacy practices for
18 the consumer.

19 A good example is the White House YouTube tool
20 where YouTube has the option for any video embedded
21 without that instant cookie, as opposed to a delayed
22 cookie. I'm not sure it's actually called an instant

1 cookie.

2 On the question of notice where this all started,
3 I think people are -- agencies need to put the
4 notice in such plain language, clearly on the front
5 page of Facebook -- earlier today the FEMA site, the
6 FEMA Facebook page that was showing, had the notice on
7 the information page of the Facebook and said, now
8 here's what we're doing. I think that's important
9 because establishing trust with the user around that
10 kind of transparency and those kinds of practices is
11 going to be key for engaging citizens in social media.

12 Moderator Landesberg: Great, thank you.

13 Jonathan, let me turn to you for just a moment
14 and ask, as our Government privacy expert, the only
15 one on the panel at the moment who is a Government
16 employee besides me. How would you describe the
17 potential privacy impacts of Government's use of
18 social media?

19 Mr. Cantor: Well, I think my colleagues up here
20 on the panel have done a pretty good job of outlining
21 some of the major ones and some of the potential risks
22 that are present, and some of the legitimate concerns

1 that are out there. Let me preface my comments with
2 the important preface of every Government person, that
3 these are my comments and not the comments of my
4 particular agency. Like a lot of agencies, we're all
5 still in this place where we're trying to figure
6 things out. Different agencies have kind of moved in
7 different directions. Some are a lot more comfortable
8 than others and have started to experiment more than
9 others and some are very hesitant to get too far out
10 there. My agency is one of those one's that is rather
11 hesitant to get too far out there right now.

12 Lillie, you pointed to the unique thing about the
13 fact that every agency has a different mission and by
14 different missions sort of bring a different set of
15 problems.

16 So, for example, at Social Security, a lot of our
17 transactions are very specific to the individual.
18 They're benefit related. There is a lot of personal
19 information involved and there is a kind of a natural
20 concern about having people put personal information
21 out there unintentionally, especially, when the key to
22 anything we do is the Social Security Number. That's

1 what it was for and so we have that concern. So,
2 there is sort of that need to proceed cautiously.

3 Not every agency is in that position because
4 their services are more generic and more widely
5 available.

6 Getting into the privacy impact, I mean, there
7 has been a lot of comments on the Fair Information
8 Practice Principles; The Privacy Act, that framework
9 that has been in place for a long time, and really
10 when you look at it, those are the places where the
11 potential for privacy impact really lies.

12 I think I agree with most of my fellow panelists that
13 one of the keys to make this possible, if we're going
14 to do this and use it as a tool to allow communication
15 with the individual, and I agree that the Government
16 is not an equal to an individual, but if you're going
17 to try to move into that model where you are
18 communicating, trying to make that information more
19 available to individuals through this channel, then
20 it's really important to rely on very, very, clear,
21 very well written notices.

22 These are huge challenges, but there are things

1 that need to happen; very, very, strong opportunities
2 for people to exercise choice and to try to develop
3 methods to exercise that choice to approach the
4 service providers in ways that they may be willing to
5 work with us on provisions of those terms of service,
6 and to minimize to the absolute point necessary.

7 You're right and many of these things where it's
8 just a push it should be like Danielle said a one-way
9 mirror. If you're just pushing and you're not
10 interested in collecting anything and you don't even
11 necessarily care about the comments and feedback, then
12 don't even bother. Some of these sites allow settings
13 where you can't even comment on them. If you don't
14 care then don't use it. If it's just another channel
15 for broadcasting then use it that way. If you're
16 going to collect comments, do you really need to know
17 who made that comment or is it more important to just
18 understand what the comment is?

19 This isn't a policy-making site where you're
20 going to, for example, arguably trying to issue a
21 regulation, you're just interested in what the public's
22 reactions are to your video or anything like that.

1 Then do you really need to collect the comments and
2 have any sort of correlation between who sent it in?

3 Once the Government tries to suck that in, you
4 get into a much more Privacy Act voyeur, you know,
5 Federal records have to regulate its structure, but
6 the issue is you get into what the third-party is
7 doing with that information, and you just need to work
8 as clearly as possible to make it clear to the
9 individual that, at least from the government's
10 Privacy Act's point of view -- I like that term. I
11 don't know if I would put myself there; but hence, a
12 key driver is really making sure that the individuals
13 and members of the public understand the distinction
14 between an agency's Facebook page or agency's YouTube
15 page or their accounts there, and the agency.gov
16 Web site, which is where that secure transaction --
17 because it's not always clear to everybody and
18 especially, it's a really complicated issue with a lot
19 of the branding that we have been talking about
20 earlier this morning, that you need to make it really
21 clear.

22 So, all of these things kind of have to be

1 embedded in that notice and everything has to be as
2 clear as possible. Of course, you don't want it to be
3 500-pages long, because you want somebody to actually
4 read it. So, the challenges there, it's huge, but I
5 can say at least as a privacy professional in the
6 Government, these are the things that we're wrestling
7 with and trying to push out there to guidance to
8 agencies to use as they approach the issue.

9 Moderator Landesberg: Thanks Jonathan.

10 This is a question for all you. What do you
11 think the Government's role should be in educating the
12 public about all of these issues?

13 Anyone want to take a crack at that?

14 Mr. Stanley: I do think that if the Government is
15 to engage in a particular social networking company
16 that they do have responsibilities above and beyond
17 anybody in the private sector, because in some ways
18 and at some level it implies an endorsement of that
19 company. Presumably, the Government would not get
20 itself involved with some really shady company. So,
21 you get a lot of the practices that are going on in
22 the Internet advertising space that are quite shady.

1 I think that the Government does bring upon itself,
2 you know, some responsibility to really educate people
3 even about things that they may be doing on a regular
4 basis in their normal lives outside of the Government.

5 When you're dealing with the Government, the
6 Government should really help -- should have an
7 affirmative role in trying to educate yourself, you,
8 about what you're getting into; precisely, because the
9 power relationship is different with the Government.

10 Moderator Landesberg: Thanks Jay.

11 Let me just ask. Are you all in the back still
12 having trouble hearing us?

13 Audience: Yes.

14 Moderator Landesberg: Oh, sorry.

15 Audience Speaker: When you guys talk to or when
16 you talk to each other, like turning your heads, we
17 can't hear you very well.

18 Moderator Landesberg: Okay. Sorry. I wish you'd

19 --

20 Audience Speaker: Just speak up.

21 Mr. Cantor: Sorry about that.

22 Moderator Landesberg: Okay, we'll do better at

1 that. Thank you.

2 Does anybody else want to -- oh, Heather, go
3 ahead.

4 Ms. West: I mean, Jay, largely said what I wanted
5 to, but I think the Government does have a huge
6 opportunity to educate the public around these issues,
7 and saying, some of this content on this page
8 originates from "Provider A," and should go look at
9 their privacy policies, and to go see what they're
10 doing. You can follow this link and really educate
11 the users that when they go to Facebook, they're not
12 just getting content from Facebook.

13 Ms. Coney: I think that it's important to define
14 when -- especially, Government agencies, because you
15 do have formal rule-making processes that require the
16 collection and use of information in a particular way.
17 You can use your Facebook or Twitter or MySpace, other
18 accounts, to kind of engage people and let them know
19 about opportunities, and how the Government agency
20 actually works.

21 Drive them through to the official sites where
22 comments are made and will become a part of this

1 delivery process. Make sure people understand the
2 difference between, oh; you can comment and engage us
3 here in this social networking environment. That we
4 protect your privacy in this way, so that people can
5 differentiate between, oh, I'm on a Government
6 sponsored site that's on a social networking
7 environment. This is a quality of the engagement and
8 this is what is being done to protect my privacy, and
9 this is another aspect of the Government's -- that
10 agencies work, and it's telling me to go to its
11 official site, because that is where you need to go in
12 order to have your voice heard, and in the
13 deliberative process, and what that means for the user
14 to participate in that process. It would be a great
15 way to educate consumers, not just about social
16 networking and the quality of the engagement with
17 entities in that environment, but also about the
18 activities and what that Government agency actually
19 does in people's day-to-day lives.

20 Moderator Landesberg: Thanks.

21 Danielle?

22 Ms. Citron: Peter Squire had an excellent

1 question, and Peter, yeah, you're here, right? So, I
2 can reference your question before --

3 Peter asked will Congress be acting in the space
4 and making policy, and I think that, we know, that law
5 plays a powerful educative rule. Should Congress or
6 even agencies engage in policy making? They can use
7 that as a wonderful opportunity to educate the public.
8 These privacy issues, maybe we don't need Congress to
9 do it, we don't. We're agencies and we engage in rule-
10 making or even policy statements that we can publicize
11 endlessly, right?

12 Moderator Landesberg: Thanks.

13 Anything else to offer?

14 Mr. Cantor: Yes. I mean in answer to the
15 specific question about whether or not we should
16 engage in actual education, I think that what I would
17 -- at least, some of us in Government who are trying
18 to work on this issue, we feel that helping educate
19 people is an inevitable part of our role. By inviting
20 the public on to these types of forums where the
21 business model originally designed was so very
22 different then interacting with your Government that,

1 the risks that we're up here talking about, and that
2 this session is about generally, it almost
3 necessitates that clearly there is a need to educate
4 people a little bit more or a lot more, depending on
5 the situation, to what's going on and how these sites
6 work. Because when you move into interacting with the
7 Government, unless it is a straight push, there is
8 such a difference. I mean, I agree with the points
9 that everybody has raised about the power
10 relationship. It's just not the way that these sites
11 were designed. The way that they were developed was
12 so that people could chat with each other socially.
13 What's going on is a much more official type of
14 transaction and the rules may change. They may be
15 different than that chat type of thing. You don't
16 chat with, you know, the President. You don't chat
17 with him in the same way. So, it is important that
18 people understand those differences and it's incumbent
19 on the Government, as the entity, trying to push
20 content to these sites to at least make that
21 distinction clear.

22 Moderator Landesberg: Thank you Jonathan.

1 Anybody else care to chime in on this point?

2 (No response)

3 Moderator Landesberg: Okay. We've reached the
4 point now where we would be happy to take questions
5 for the panel. If you are interested in doing so,
6 please approach the mike here and we will -- let us
7 know who you are, please, and your affiliation.

8 Mr. Ferron: Bob Ferron, USCIS.

9 One of the points that I'm not hearing you make
10 is the differentiation between internal and external
11 uses of the social media. I think I'd like to hear
12 the panelists certainly address that.

13 The other, in response to some of the panelists
14 saying the Government provides benefits of many sorts,
15 part of the issue, and again, it came back to my
16 comment this morning on the -- management, is if we
17 want individuals to be able to access their private
18 information, to protect their own information, to give
19 redress to the harms that they feel they are having?

20 We're also going to have to come up with a
21 mechanism to allow them to assert their identity in a
22 way that we can understand; we're not giving out

1 private information to the wrong person.

2 I'd like to hear the panelists comment a little
3 bit on that as well.

4 Moderator Landesberg: Would anyone like to take
5 that question.

6 Mr. Cantor: I'll, at least take a crack at one --
7 I mean, I'll take a shot at both pieces of it.

8 At least on the internal users; so, in other
9 words, an agency having some sort of collaborative
10 social forum within itself, there are opportunities
11 that are available internal to an agency to deliver
12 notices and practices about how the site works.
13 What's appropriate and what's not.

14 You start to get away from some of the official
15 First Amendment-type issues that folks have talked
16 about this morning, when you're internal to the agency
17 and it's being used within an agency for an internal-
18 policy development forum or discussion about a
19 particular issue. Because at least in that sense,
20 it's all in the house and so the ability to
21 communicate is there through other tools, in addition
22 to that.

1 I can't, as an agency official, reach everyone
2 who might need to interact with Social Security at
3 some point outside. That's not necessarily the case
4 with an internal discussion. I'm sure you know that
5 the Secretary or the head of USCIS has the ability to
6 reach all employees of that agency about some of those
7 things that can be written up. You can have your legal
8 counsel review it. You can put everything nice and
9 neat. You can put it up on that form. It's just --
10 it's a very -- there are some, I guess, pieces of that
11 that are different, at least conceptually. Then, of
12 course, the other thing is you probably wouldn't be
13 having the same type of discussions.

14 Again, we're not using these things internally
15 right now, so I don't have as much experience. But
16 when imagined, you set up a forum and it's much more
17 of an internal business forum for trying to accomplish
18 a specific business goal might be a little different
19 than the concept of someone who might not be -- you
20 have much different levels of understanding of what
21 the media are and the general public, and sort of the,
22 perhaps, purpose of the discussion we heard sort of

1 splintered conversations a little bit about those this
2 morning.

3 So, I do think there are differences and, of
4 course, differences that impact expectations, but if
5 it is an internal forum, you are doing all the
6 collection internally. If you are collecting and
7 storing that personal information, the Privacy Act is
8 going to apply the -- FOIA is going to apply, so you
9 get into a much different legal framework, at least
10 the way that I see it.

11 So, it is something to keep in mind with that
12 side.

13 Ms. West: I'd like to pipe in and echo that.

14 When the information is held internally, all the
15 privacy protections around other Government
16 collections of their employee information are going to
17 apply and then -- so that seems a lot less
18 problematic, because those protections are, at least,
19 partially in place.

20 Moderator Landesberg: Peter?

21 Mr. Squire: Thanks; Peter Swire, Ohio State
22 University and Center for American Progress.

1 This actually picks up, I guess, a little bit on
2 this. Do it on site versus third-party. Let me ask
3 the question this way, because in a privacy panel the
4 pretty strong message was, don't do it in third-party
5 providers unless they have all the safe guards in
6 place. That's what I think I heard from Jay and
7 Danielle.

8 Now, I'm going to ask the question this way, in
9 terms of agencies experimenting with these things.

10 There is a whole series of rules. There are
11 Section 508 Disabilities Rules. There is Privacy.
12 There are Records Act Rules and a lot of others that
13 we'll talk, tomorrow, on the legal panel.

14 If you say to the Federal agencies, you cannot
15 use any of these technologies until of this is fixed
16 on site, then an awful lot of this morning's panel
17 wouldn't have been able to display; right? An awful
18 lot of it wasn't fixed on terms of use
19 before experimentation happened. So, is your
20 position don't experiment until you fix all of these
21 things? Because I think a lot of people who are
22 trying to build this in agencies, want to comply with

1 the law and also want to try new things that are
2 exciting and advance the mission of the agency, and
3 are trying to struggle, then, with the real clear
4 message that if you do it in third-party places, you
5 get freed up from some of these burdens and you can
6 actually try things, but then the privacy and the
7 other concerns are there.

8 Maybe for Danielle and Jay, because you sort of
9 clearly said, don't do it until you have the full
10 privacy protections in place. What do you say to
11 managers who are trying to figure out how to
12 experiment here?

13 Ms. Citron: I'll take that.

14 I think, just to clarify my point, I would love
15 to see experimentation, but there should be a stead-
16 fast rule that Government agencies can't give this
17 information to law enforcement. We can't control what
18 third-parties do. So, like any other user, we can't
19 control what Facebook does with our data unless we
20 freak out when they change their terms of service;
21 right? But I think we should permit Government to
22 experiment, but on the proviso that they're not going

1 to use the information -- what's written on my Wall,
2 what I muse on my little mini-blog on Facebook or
3 MySpace. They're not going to look at it for law
4 enforcement purposes or to remove me -- you know, for
5 the Federal Parent Locator. So, I think we can
6 actually slice the apple in half.

7 Mr. Squire: So, a Federal agency and its own
8 privacy policy could say, and we're not going to seek
9 this information from the third-party site except --

10 Ms. Citron: Right.

11 Mr. Squire: -- in whatever the narrow list is?

12 Ms. Citron: Right.

13 Mr. Squire: Agencies could say that without
14 having to get terms of use agreement from Facebook or
15 something?

16 Ms. Citron: I think so, but I'm making a set of
17 assumptions and perhaps I'm wrong. But it's possible,
18 yeah.

19 Mr. Stanley: I'd echo that and I'm very
20 sympathetic to what it must be like in a Federal
21 agency trying to be loose and stay with the times, and
22 yet, be hamstrung by all these rules and the damn

1 privacy advocates and all the rest.

2 (Laughter)

3 Mr. Stanley: So, I'm of two minds. On the one
4 hand, yes, you should follow all the rules. The
5 ACLU's position is the law should be followed. We
6 think that privacy is very, very important.

7 On the other hand, approach it mindful of privacy
8 and don't do anything that you wouldn't want done to
9 you. Don't start collecting masses of data on your
10 users and making them available to national security
11 agencies when you're -- you know, get the big stuff
12 right and then as you go through time, then you can
13 work out the little stuff.

14 I guess that would be my answer.

15 Mr. Jones: I would like to see the energy around
16 modernizing Government Web sites right now and making
17 use of third-party services on Facebook and YouTube
18 and whatever. I'd like to see some of that energy go
19 towards improving the terms of service policies of
20 those services, because they are flawed right now. A
21 lot of it is just completely vague and hidden about
22 how this information is being used.

1 There are two sentences in YouTube's Privacy
2 Policy that says, well, we can use this for
3 advertising or serving custom content, but you really
4 don't know what Google's doing with your data, once it
5 gets it.

6 I think there is a stronger expectation of
7 privacy when you interact with the Federal Government
8 then there is if I'm, you know, ordering a pizza
9 online. I understand that there are challenges here
10 and you want to make the full use of these cool, new
11 technologies.

12 I think the policy needs to be reformed. My
13 understanding is, to some degree, it is in the process
14 of being reformed. In the process of that, we can't
15 throw the baby out with the bathwater here though.
16 There is an enormous amount of money for these
17 companies and partnering with the Government. I think
18 that the Government should set some standards that
19 they have to rise too. I think that's not only going
20 to help those sites and help the Government, it's
21 going to help other organizations that -- frankly, I
22 think in a lot of cases, people deserve the same

1 privacy protections when interacting with groups other
2 then the Government. This is a point at which we can
3 improve those things.

4 To Government webmasters, I'm not sure what to
5 say working in the current context. To people who are
6 working on the policy, I think -- well, working as
7 having noted on policies that haven't been updated for
8 the new era and the way technology works today.

9 Mr. Stanley: Can I just add, I think that the
10 current status quo that the Government Web managers
11 want to become part of is in some way a corrupt status
12 quo and that may become apparent over time in ways
13 that it hasn't now; in the sense that, privacy is not
14 being protected and people are not thinking about it,
15 and they don't seem to care. But, eventually these
16 things will become -- a lot of issues that are
17 currently buried will come to the fore and it will be
18 much worse in a Government context when they do then
19 in the private context.

20 Ms. Coney: I would add one thing.

21 We want to be sure that when we talk about fixing
22 the Privacy Act, that we don't try to fix it by making

1 it technology dependent. That whatever policies are
2 put into place, they have to be technology neutral.
3 It's about the collection and use of personally
4 identifiable information.

5 Now, the definition of personally identifiable
6 information is radically changing because of online
7 behavior. We're talking about IP addresses. We're
8 talking about handles. We're talking about email
9 addresses. We are talking about how someone might
10 navigate a particular page that may identify them in
11 ways that we, right now, may not be fully aware of.

12 So, a couple of things; no commercialization of
13 information that is collected on your social
14 networking sites, that people are encouraged to report
15 when they think something has been inappropriately
16 used based on their navigation on a Government site,
17 where they maybe getting ads and so forth. And, that
18 you manage the ad space and how ads are being used.
19 You manage how other technologies like Widgets might
20 be used and what information they might collect; that
21 you constantly review that and you try to improve
22 that, and you make sure that process is as transparent

1 as possible, engaging the social networking community,
2 as well as experts within the agency, to try to make
3 the agency smarter about the privacy protections that
4 it can provide on line.

5 Moderator Landesberg: Thanks, Lillie.

6 Danielle, do you have one last -- I'll just let
7 Danielle and then Tim.

8 Ms. Citron: So, I guess just to recap for Peter's
9 question. I think that in Government's use of third-
10 party social networking sites, I'm hopeful that we can
11 have a policy of data collection minimization and when
12 it comes -- these are the personal information, which
13 of course, we'd have to work through how we define it
14 and a policy of data will maximize data flow when
15 these are the policy discussions, that we can bridge
16 those two and bring them -- marry them. The privacy
17 and transparency actually run in the same direction.

18 Moderator Landesberg: Thanks.

19 Tim?

20 Mr. Jones: I just want to add that in addition to
21 sort of encouraging -- perform of a lot of the terms
22 of the service of these companies, I think the

1 Government is in a really good position right now to
2 encourage the development of actual new technologies.

3 I'm much more of a technologist than a policy
4 analyst. You know, a lot of the problems are that the
5 tools just do not exist to handle, say, something like
6 Web analytics in a way that it's fully anonymized and
7 privacy sensitive. In theory it could, it just hasn't
8 been built, because there is not a strong corporate
9 funded demand for it.

10 Certainly, Google could build -- it got --
11 they're good at solving tech problems. They could
12 build a way for you to track what's happening to all
13 your information. They've actually taken some great
14 steps in that direction. So, I'm hoping this is an
15 opportunity to encourage them and groups like them to
16 continue to do that.

17 Moderator Landesberg: Thank, Tim.

18 If you'll bear with me for a moment, I would like
19 to exercise my moderator's prerogative and ask one more
20 question and then we will get to yours.

21 It's really for you Jonathan.

22 What privacy risks are posed -- oh, sorry, wrong

1 question, wrong page, long day.

2 What's the Federal Government doing, generally,
3 to address the privacy impacts that we're hearing
4 about?

5 Mr. Cantor: Well, it's interesting that this
6 discussion happened because this sounds like a lot of
7 Government privacy professionals getting together in a
8 room and we all start asking questions and they flow,
9 and then some of these meetings that we've tried to
10 have, they've gone two hours, more than two hours
11 where, people are constantly coming up with the same
12 discussions. I think what we've tried to do through
13 the auspices of the Privacy Committee, the CIO
14 Council's, we've tried to actually begin a conversation
15 where it's not every agency trying to figure it out on
16 their own. So, we're starting to cross-leverage each
17 others resources, starting to talk to each other,
18 brainstorming ideas. Everybody's been really
19 supportive and we're coming up with a lot of good
20 ideas. What I'm very happy to hear is that some of
21 our ideas sound a lot like some of your ideas, where
22 we're starting to think about combining the resources

1 of the Government differently and approaching the
2 problem in a different way, that I'm not sure any one
3 agency on its own would have been able to do.

4 If you come from a small agency you're not going
5 to approach the behemoth that is Google, and I'm not
6 singling them out, most of these companies are large
7 and they're commercial; they're driven by profit, that
8 you need to come at them from a position that makes
9 sense to them in a way that you can work with them,
10 but at the same point in time, they recognize your
11 unique needs. That's going to work much better as a
12 comprehensive approach, as opposed to a disjointed
13 agency-by-agency approach.

14 So, these discussions are going on and, of
15 course, we're running very, very quickly to try and
16 keep up with everybody's desire to experiment and try
17 new things. So, there are discussions going on within
18 Government and, yeah, we're all trying to work
19 together collaboratively.

20 Moderator Landesberg: Thank you, Jonathan.

21 Please?

22 Ms. Bloomenthal: Hi, I'm Danielle Bloomenthal

1 from Public Affairs at U.S. Customs and Border
2 Protection. I have a comment and a related question.

3 Maybe this is the Generation X'er, in me, but
4 when I go on to Facebook or YouTube, I have zero
5 expectation of privacy at all. I mean, I really think
6 that my data can be tracked anytime, all the time, and
7 I just don't have that image in my mind that it is
8 private. So, I'm not sure why the Government should
9 go to all this effort to try and make these commercial
10 organizations transform themselves into replicas of
11 us, when they never will be.

12 Frankly, they're started by 23 year olds, 29 year
13 olds, who just don't know and don't care. That's part
14 one.

15 Second part of the comment is that I don't
16 understand why the Government can't just get together
17 and copy what all of these social networking sites
18 have done in ways that make our own standards work.
19 So if, for example, we want to protect women from
20 being stalked by violent partners, we then create a
21 site that will allow them to network socially that
22 doesn't pose that kind of a risk, and so-on and so-

1 forth.

2 So, the question is, do you think that we can
3 come up with an IT speak, like a business
4 requirements document for privacy, that we would then
5 apply to such a comprehensive solution that any agency
6 could use, and Public Affairs folks, like me, wouldn't
7 have to try to figure out all the technicalities?

8 Moderator Landesberg: Who would like to answer?

9 Mr. Jones: Can I?

10 Moderator Landesberg: Go ahead, Tim.

11 Mr. Jones: I think I would love to see that sort
12 of thing and it may not -- what might be even more
13 efficient is to have a document and this maybe goes to
14 your first point, what might be more efficient than
15 the Government trying to build its own service, is for
16 the Government to set out clearly what the
17 requirements are, and then to encourage private
18 companies, the 23-and 29-year olds that you're talking
19 about, to build services to those specifications.

20 In the end, I think we've seen the -- these
21 companies have come from this corporate start-up
22 culture and I think there are 100-new social

1 networking startups being launched every week. I
2 think if you let a 100-flowers bloom every week that
3 meet that privacy standard, that's probably going to
4 be more effective and less expensive than the
5 Government trying to do its own thing. I think that
6 goes to your first point too, that these sites should
7 have better privacy protections than they do.

8 I think you're smart not to expect a huge amount
9 of privacy, but there is a lot of -- there is a
10 difference between being realistic about your personal
11 interactions and then saying, well, what should things
12 be?

13 Moderator Landesberg: Danielle?

14 Ms. Citron: Danielle. For your first questions
15 about, do we want to transform third-party social
16 networking sites, then I think the answer is no. We
17 don't want to, but we just want to set clear policies
18 for what Government can do with the information once
19 it gets it and, presumably, then is covered by the
20 Privacy Act, if it were to keep it and process it and
21 use it.

22 Ms. Bloomenthal: Okay.

1 Ms. Citron: I think we've seen the marketplace
2 respond in a way that reflects the intuition of the
3 one-way mirror; which is, Facebook and its fan pages.
4 So, I'm not quite sure if we're kind of, out to launch
5 in terms of the quote who said this, "Privacy is dead,
6 get over it." I'm not really sure that the
7 marketplace is really responding in that manner.

8 I think, to your second question about, why
9 should we care about our privacy, we know, if there is
10 none, I think the whole reason why we're having this
11 conversation is for that wonderful January 21st memo,
12 where President Obama says, we want you to be more
13 involved in Government. We want to collaborate with
14 you. We want to garner your expertise and part of
15 that is that that deal, I think he is going to strike
16 with us, is that we're going to be so excited to
17 engage, as long as we know that you're not spying on
18 us in the way that the U.K. directive so provides.

19 So, I think just as a normative matter, we're
20 going to have more people participate if, indeed, we
21 set forth pretty clear policies that are privacy
22 protective of personal information.

1 Ms. Bloomenthal: And I think that makes total
2 sense. I guess the subtext of my comment is that I
3 think the Government is a little lazy. You know, we
4 kind of want the private sector to do it for us and
5 then we want to come back and complain at them, and
6 say that they're not doing it right. I think there is
7 enough talent in the Government to create what we
8 want, that meets all the standards that we want, and
9 on top of that, to create open-source code or whatever
10 IT stuff is needed so that any developer can come in
11 and create a social networking site easily that meets
12 those terms.

13 Mr. Stanley: I think I would also dispute the
14 implication of your comment that like, anybody who is
15 under the age of 30 doesn't care about their privacy -
16 -

17 Ms. Bloomenthal: Well, that's my observation --
18 (Laughter)

19 Ms. Bloomenthal: Talk to my daughter.

20 Mr. Stanley: They might seem that way, but
21 teenagers are going through identity formation and all
22 kinds of things.

1 I think neither the companies involved, nor many
2 of the people on them, consider that if you put up a
3 Facebook account, you've given away all privacy
4 interests and whatever goes up there. But, I mean,
5 you're certainly safe if you make that assumption.
6 For you, that's great, but I don't think that the
7 world shares that necessarily.

8 Ms. Bloomenthal: Okay.

9 Moderator Landesberg: Thank you.

10 May we have the next question please?

11 Speaker: Actually, I come back to the question
12 with regards to the generational difference.

13 As a sole professed Millennial, I'm just
14 wondering if it's not necessarily that we don't
15 necessarily care about privacy, but we care about it
16 differently, and that we see that, perhaps, innovation
17 and the benefits of innovation far outweigh some of
18 the privacy concerns or at least they're equal.

19 So, I just wanted to know, for example, if you
20 see in your discussions in the myriad of discussions
21 and conversations about this, if you see that there is
22 somewhat of a generational evolution in the

1 discussions of privacy and how the public is starting
2 to perceive privacy, especially it's those in my age
3 groups, start to become you and start to become
4 Government workers who are going to oversee these
5 policies?

6 (Laughter)

7 Speaker: Because we will be coming. We are
8 there.

9 That's my first question.

10 Second question, with regards to friending my
11 good friend Barack Obama, who I am personally,
12 actually quite or both -- I wanted to know with
13 regards to certain agencies, for example, that do
14 empower individuals, particularly within public
15 affairs, to represent the agency on an individual
16 level. Cause an case example is Andrew Wilson during
17 the salmonella peanut recall at HHS; he was blogging,
18 as Andrew Wilson on Twitter, for example. I was
19 wondering, for example, do all of the policies and the
20 compliance issues that you're talking about change as
21 agencies start to empower individuals to speak on
22 their behalf? In particular, for example, Bob this

1 morning at TSA or for example, John Shea known in FEMA
2 quite universally as kind of an innovator in that
3 space. But he is known, individually, from that
4 organization as being sort of the representative of
5 that kind of social media engagement.

6 So, I just wanted to know from an individual
7 level, does it change?

8 Ms. Coney: I think that is a good question
9 because this is part of the discussion that has to take
10 place.

11 When someone is officially designated to be the
12 public voice or the public face in the event of a
13 crisis or a problem or just sort of the person who is
14 going to be leading the blog discussions, that's one
15 thing, but as Government employees, you have personal
16 lives and you go out there, and you do your own thing.
17 Some have even been in social networking environments
18 for a very long time.

19 Do you want to have to register with your agency
20 that you have a page, and if you're not carrying out
21 discussions that have anything to do with your job?
22 You have social contacts that have nothing to do with

1 your work and people may or may not know what your job
2 is, and what agency you work for. So, some of these
3 discussions are going to have to happen in contexts of
4 what the relationship is, what it's intended to do and
5 so forth.

6 I was looking at currently what is going on in
7 Iran. There are lots of individuals who are online,
8 who are engaged in their own form of free expression
9 and offering advice or tips or whatever. We're not
10 asking questions about who is doing what.

11 The Government of Iran thinks it's the official
12 U.S. Government's acting, when we know, in fact, it's a
13 bunch of individuals acting. But what happens if the
14 State Department has a position about our citizens
15 engaging in social networking activities regarding a
16 country? We might have relationship with a policy
17 position with or something like that. What happens
18 then? What happens when it's other interests that are
19 being impacted by online activity?

20 If we don't lay the foundation for policy right
21 now and think in terms of what we think is appropriate
22 and what we think is inappropriate, and that the

1 agencies' level of engagement of social networking is
2 to push information; not necessarily to do anything
3 else with the fact that they have these relationships
4 with social networking companies, we need to talk
5 about those things now. Because, at some point, we
6 might get to a point that, as an individual, is it
7 appropriate because you have network-relations online,
8 for the agency to have any say over that? But if you
9 officially are engaging in agency activity, that
10 should be transparent to those who you are connecting
11 with.

12 Moderator Landesberg: Thank you.

13 Jonathan?

14 Mr. Cantor: Just to build on Lillie's comments, I
15 mean, they were excellent and pretty comprehensive
16 about some of the issues that are present there and
17 sort of the distinctions of where and when, and then
18 how do you set up rules of behavior? Again, you're
19 dealing with the framework that was built in a
20 different time, different set of expectations. So, if
21 you're thinking, for example, about the government's
22 ethics rules, you know, do you really want to have

1 policies out there that require every Federal
2 Government employee to say, kind of like I did when I
3 first began making my remarks; these are not the
4 official positions of my agency. These are my
5 personal thoughts. I mean, you may have one of those
6 people who have been in that position, who is going
7 back and forth. You get sort of a mixture of
8 issues. You can get into records issues; with that,
9 when do they become records of the agency? When are
10 they your personal notes? And it goes on.

11 I'm sure some of that will come up in tomorrow's
12 panel because there is sort of a blending there on the
13 legal issues.

14 On your first comment though, you made a comment
15 about generational issues. I come from the Social
16 Security Administration, which is definitely an agency
17 in the U.S. Government that tends to target older
18 people, so Boomers and older, just because of the
19 nature of our business. We do have interactions with
20 people younger than the Baby Boom Generation, not just
21 within the employees, but there is a definite trend
22 that we've noticed just, for example, in Web site

1 adoption. Even the comfort with visiting a regular,
2 you know, SSA.gov, kind of thing, is a huge
3 distinction between the generations. It's not as
4 extreme as one might think, but there are differences
5 between what people are comfortable doing and the
6 types of transactions.

7 Moderator Landesberg: Thank you, Jonathan.

8 Our last question, please?

9 Mr. Alnite: Well, I guess it gets to -- Lou
10 Alnite, DLA.

11 The question that has to do with generational
12 differences and the fact that in MySpace and Facebook
13 you have preferences and privacy that you can select
14 to share your information with select groups, and many
15 individuals are comfortable with that concept.
16 However, I don't think we're going to see any time
17 soon the privacy preference selection of say, police
18 or Federal Government or perhaps, we will. But, I
19 don't think we will see it with the intelligent
20 services or things like that. So, I think there is a
21 distinct power differential that you're going to see
22 when we're sharing information as was pointed out, and

1 that's sort of the issue with social networking that,
2 if you make it that simple for individuals to
3 determine who they are sharing their information with,
4 the choice of permitting my information to be shared
5 with those individuals, which a lot of these younger
6 kids get, they'll opt out of sharing.

7 Moderator Landesberg: Thanks very much.

8 Well, we've come to the end of this panel, which
9 has laid a fantastic groundwork for what follows in
10 the workshop.

11 I hope you join me in thanking our panelists.

12 (Applause)

13 Moderator Landesberg: We will now take a 15-
14 minute break. I hope you will all be back here at
15 3:00 for the panel on security issues.

16 Thanks.

17 (Recess at 2:45 p.m.)

18

19 Panel 3: What Security Issues Are Raised by Government
20 2.0?

21 Moderator Crane: Welcome back. There are
22 certainly many aspects with this panel, I hope you'll

1 get; but, one key take away is certainly you'll get
2 technology I hope you'll use as looking at how do we
3 enable use of Web 2.0 technologies in Federal space
4 while considering the security aspects. Security is
5 the enabler, not the naysayer saying no; so,
6 hopefully that's what we will see today and discuss as
7 what are the difficult issues and how can we work
8 through them to enable the secure use of Web 2.0
9 technologies and information systems. I also have an
10 announcement to make. I don't know how many of you
11 have heard that Web 2.0 is now the one millionth word
12 in the English language. How many of you have heard
13 about that? Look, about twenty per cent of the room.
14 So, for those of you who didn't know, a little
15 group called the Global Language Monitor has a utility
16 that looks at the number of words on a Web site and we
17 saw that Web 2.0 made the threshold on June 10, 2009
18 at 5:22 in the morning, EST, and as far as they're
19 concerned, it became the one millionth word in the
20 English language. Now, the Oxford English Dictionary
21 was quick to comment that they're a little bit
22 skeptical on their methods; so, I'm not sure if that's

1 going to be adopted any time soon. Apparently, noob,
2 was the 999,999th word, n-o-o-b. To clarify a little
3 bit of the technology, this is one thing that pops up
4 as a confusion point; when you look at Government 2.0,
5 why we're here today, is roughly defined as embracing
6 Web 2.0 technologies throughout the Federal
7 Government; so, we then get into Web 2.0, which we
8 covered using the Internet as a platform and then some
9 of the areas I want to talk about today or have our
10 panel talk about today are looking at social media and
11 cloud computing. You can see there are a lot of areas
12 of Web 2.0 that we might not necessarily cover; so,
13 it's a big world when you start talking about Web 2.0.
14 A lot of confusion gets around that. Social media,
15 which we've covered a lot today, includes Web site and
16 communication and collaboration through online social
17 networks and then cloud computing, using the NIST
18 working definition of convenient on-demand network
19 access to a pool of configured resources that can
20 rapidly be provisioned, composed of five essential
21 characteristics, four deployment methods, and three
22 delivery models Say that three times fast. That's

1 the space we want to play in today. One of the key
2 things that gets into security when we look at Web 2.0
3 is that the threats that you deal with at home are not
4 the same as the Federal Government is faced with and
5 that's most easily stated when you look at the Hill
6 testimony back on May 19th from our acting CIO, Margie
7 Graves, where she provided this statement in her
8 testimony: "We have now learned first hand about the
9 growing category of threats that directly target
10 Federal systems and our information. We have also
11 witnessed how these threats have become more
12 persistent, more pervasive and even more aggressive
13 than we had imagined. These actors appear to be highly
14 motivated and well-resourced and will take all of our
15 collective efforts to keep them out of our networks."
16 So Facebook for a Federal employee, Facebook for a
17 public network is not the same thing as your kid
18 accessing from home. That's one of the key points
19 that I want all of you to understand; so, that being
20 said, why is Web 2.0 different from Web 1.0; in short,
21 Web 2.0 is using the browser as an application, not
22 just a reader; we are accessing a lot more avenues

1 that have a lot more avenues and vectors for attack.
2 Web 2.0 relies on user-generated content; that's the
3 entire concept of Web 2.0 user-generated media. Web
4 2.0 has a feature in which applications in content,
5 using those advanced Web 2.0 technologies, more than
6 just viewing it as a browser; so, with that brief
7 introduction, I want to go into our panel discussion.
8 I also want to put a plug-in for Dr. Drapeau and Dr.
9 Wells; their paper was released back in April of this
10 year and I think you are going to be provided this
11 link or you can just Google it. Mark, do you want to
12 say anything about your paper?

13 Mr. Drapeau: No.

14 Moderator Crane: Great.

15 Mr. Drapeau: It's certainly worth a read and
16 after hearing this panel, you can go in depth on this
17 link and it will provide some background and it's
18 available on the National Defense Web site, ndu.edu.

19 Moderator Crane: I second that endorsement. To
20 introductions, first, to my left, I'd like to
21 introduce Mr. Brian Burns; he's currently Chief
22 Information Officer for Emerging Technology at the U.S.

1 Department of the Navy. I'd also like to introduce
2 Mr. Dan Chenok, Senior Vice President and General
3 Manager of Pragmatics. Dr. Mark Drapeau, Associate
4 Research Fellow at the Center for Technology and
5 National Security Policy at the National Defense
6 University, Department of Defense and Dr. Edward
7 Felten, Professor of Computer Science and Public
8 Affairs at Princeton University. The format is going
9 to be that I'm going to ask some questions, the panel
10 will respond; if you guys can't hear us in the back of
11 the room, just raise your hand; we know it's not for
12 questions; it's a reminder we need to speak up into
13 the microphones. My first question to the panel is in
14 what ways could Web 2.0 actually enhance security?

15 Mr. Chenok: I'd like to take a minute before I
16 address the question as to how can Web 2.0 enhance
17 security. How many people were on Facebook or Twitter
18 in the last 12 hours? Okay and how many people when
19 you go on Facebook and Twitter accept the default
20 settings for security? How many expand them? That's
21 good; this is a savvy crowd. How many are tweeting
22 right now about this question? Very good. That last

1 point is actually a good one because part of Web 2.0
2 security and we will talk about attack factors and
3 expanding social networks and the limits they're in;
4 but, the manner of information sharing, security and
5 transparency, a mechanism by which flaws and
6 vulnerabilities are identified and resolved, is
7 quickly transferred across whatever manner of network
8 we're talking about, whether it's network organization
9 or the Government as an enterprise is made manifestly
10 more efficient in a social network type environment;
11 so, if everybody's in a type of user group with
12 similar privileges and we know that whether it's a
13 cloud computing scenario, public or private cloud
14 scenario, where you could push a patch out immediately
15 to the entire network or whether it's a scenario where
16 you don't have an automated patch where you could
17 capture some vulnerability or threat that can
18 therefore be transferred, information shared about
19 that threat in real time, people know what to do with
20 the response, that's made much more apparent and
21 secured in a Web 2.0 type setting; it helps with
22 better decision making; It helps enable

1 collaboration about security in that sense of a
2 community combating security; there are certainly ways
3 that we can get into it about Web 2.0; but, that
4 wasn't the question; so, I'll get into the question
5 and stop there.

6 Mr. Drapeau: I didn't hear much of what Dan said
7 because I was tweeting what he said about Twitter. In
8 all seriousness, even though I was doing that, in
9 terms of how this stuff can help you, to some degree,
10 I think of it as a situational awareness tool in some
11 extent as to what I do in my personal life and to some
12 extent, that bleeds into the Government. It really is
13 a great way to tell me what's going on out there and
14 since I've become an avid user of tools like Twitter,
15 I lose old tools a lot less; I've replaced old ways of
16 doing things with new ways of doing things. These
17 tools are really good for finding out what's going on
18 at the edges and finding out unconventional sources
19 from people you don't know that can sometimes change
20 the way you think about a topic and I think in terms
21 of the Government using these tools, it fits into
22 intelligence gathering and security in a similar way.

1 We often think that we know the sources of important
2 information. We often think we know the list of
3 experts and invariable we don't, especially for
4 emerging threats. I think these tools can generally
5 be very useful; in this event we're talking about how
6 to these things safely; but, I think corporations and
7 some people in the Government are already using them
8 whether they're allowed or not; so, I think it would
9 be a good idea to move toward having an official
10 policy of using them.

11 Dr. Felten: One of the characteristics of Web
12 2.0 is in the context of the Web as a Web page; what
13 that means is the users are always using the latest
14 version of your software; they don't have to download
15 a patch; this also means if a software security
16 problems crops up you can quickly slap a Band-aid on
17 it to get around the problems.

18 Mr. Burns: From my perspective, we're looking at
19 it for the use of the sailors and marines. A couple
20 things we've noticed is that if we deploy these
21 things, we have more interaction on the personal side
22 at home communicating with families; but, the

1 interesting thing about that is instead of using e-
2 mail and forward, we can enable an internal version; I
3 call it internal weather, say Forcebook instead of
4 Facebook, we can deploy and monitor much better than
5 we can with the Web 1.0 technologies. The other thing
6 is the intelligence gathering real-time provides a
7 better opportunity as we move forward with these type
8 of tools; we can also get these tools up
9 appropriately; I think that's what Eric is working on;
10 but, it will also given us an opportunity to do more
11 thin client or capabilities where we haven't been able
12 to do it in a rapid method before.

13 Moderator Crane: Anything else from the panel?
14 Thank you. My second, what is the rationale behind
15 blocking different social networking platforms at one
16 agency but not blocking it at another agency, who may
17 be at one office building or one type of vessel but
18 not at other buildings for these mediums.

19 Mr. Burns: I'll start. JTFDNO actually put out
20 a memo in 2005 that blocked approximately a dozen
21 social networking type tools and the reason for that
22 there were some threat factors and the magnitude of

1 the change involved and the amount of information
2 warranted more control. If you think about the
3 traditional castle with a moat and a gate, the
4 security of many of the systems today, the door is
5 wide open; if you think of an 80/20 rule, it's easy for
6 the criminal element to walk in the front door and
7 take something out. They don't need to scale the
8 walls; once we get a little more sophisticated in what
9 we're doing, then they'll scale the walls and see more
10 threats than we've seen today; but, in the meantime,
11 it's important that we lock these down appropriately
12 as we go forward. I would bring back the risk based
13 approach that's being used in the Government for a
14 number of years, which means that you look at the
15 information released, independent of the agency,
16 department or program; if we look at the information,
17 the Government shouldn't decide to block it as part of
18 the whole. Even in the intelligence community, there
19 are applications to engage in social networking,
20 information retrieval, information sharing; the
21 question is the value of that information and what
22 value does the Government get in taking the risk and

1 the magnitude of harm that would occur if the information
2 were released. The Government's security log policy
3 should deal with the manner with which we approach it;
4 a lot of this will result in the risk scale; if it's
5 low, it would be you could get it anywhere from any
6 publicly available site. You could establish records
7 for sensitive information like health care records;
8 you put a significant wall but not quite as blocking
9 it but what access can the Government put on that
10 information.

11 Mr. Chenok: Tying a little bit of that together:
12 I like metaphors a lot and I like the one Brian used
13 was a moat; my co-author on the paper is a retired
14 Navy guy and he said the best risk based approach
15 metaphor is thinking about this as how a ship is built.
16 With a ship, you don't expect water to get in it; you
17 may get it in the nooks and crannies. It is built in
18 such a way that you can take on a certain amount of
19 water and still have the ship still stay afloat. You
20 can shut down some compartments and still have the
21 ship be functional. In the paper, we did a little
22 informal survey of Government agencies and offices

1 within those agencies; it wasn't scientific or
2 anything; but, it was very clear that there were
3 inconsistencies about what is actually blocked. It
4 gets pretty silly where The New York Times is blocked
5 here but not at other agencies and Twitter is blocked
6 at three but not the other ones; you can tweet grid at
7 some; it strikes me as not really a life long
8 Government employee, to ask why all the people who
9 made all the decisions are not talking to each other;
10 because if they did, they would have the same chart as
11 I have of what's been blocked indicating the x's and
12 o's; when you look at that, it just looks ridiculous;
13 maybe there are good reasons for blocking some of
14 these sites at certain places; maybe some should
15 always be blocked; but, it's not clear at all the
16 reasons for blocking these sites; there's no
17 consistency at all; frankly, the people were surveyed
18 were all scientists for the most part; so, these are
19 generally research people for the Government; so, they
20 are generally less restricted.

21 Dr. Felten: We know that arbitrariness and lack
22 of communication have been known to happen in the

1 Government; but nonetheless, there are times when the
2 omissions might make sense because of what the users
3 have been doing; I just want to add the thing about is
4 the confidentiality and availability of our CIA; sites
5 were blocked from a simple performance measure of
6 availability. The system was too large for the
7 magnitude of what we're getting; the hits or the
8 amount of hits we were getting was increasing, more
9 threats; but, it really gets down to the observation
10 was procedural, the NOC's and the SOC's, the Network
11 Operations Center and the Security Operations Center
12 seeing this come in. Procedurally, a lot of these
13 things were changed; so, you'll see a policy that says
14 thou shalt not go to this site but you can go to this
15 other one because it wasn't alive and working at the
16 time the policy was written; but, we're really looking
17 back now at the policy and being more generic so we
18 really don't have to change the policy; but, change
19 the procedures later for the sites; we're looking at
20 this from three different levels. One is, what is the
21 personal use of Government tools; what is the
22 professional use of the tools Government uses, whether

1 it is commercial or any other source and what is the
2 content filtering and deep pack analysis we have to do
3 for our inspection and content filtering that we have
4 to deploy on the type of information that we're going
5 after; so, we're really trying to step back a little
6 more to the front doors, the procedures and the
7 operations centers. A lot of agencies are not
8 catching up with these policies to make sure we know
9 what we're doing procedurally.

10 Moderator Crane: How can the Government ensure
11 reliability of information as it uses Web 2.0?

12 Mr. Chenok: I'll talk a little bit about
13 authoritative source and data.gov. The Government
14 released around ten years ago and sought to be as
15 accurate as Government information is ever accurate.
16 Having an authoritative Government source; let's say
17 data.gov and then allowing that source to be
18 repackaged and assuring that the reliability of the
19 source continues to be as pure as it can be. What Web
20 2.0 does is give the Wikipedia effect; in other words
21 so many eyes on it and if there's a problem with one
22 of the data sources, it's going to be corrected in

1 about 15 seconds; so, having the ability to provide
2 from the Privacy Act not personal information but
3 certain Government information around that
4 authoritative source is very helpful and it's enabled
5 Web 2.0 technologies in a way we haven't seen before.

6 Dr. Felten: Just to add on that, when we talk
7 about authoritative sources, tagging the information
8 in multiple dimensions, e. g. baseline content; if you
9 got out to Flickr, you're going to tag your bases the
10 way you want to tag them. But we need to really
11 expand on the FRT as a source, the location of the
12 authoritative data, the privacy and the security level
13 of that data. We really start with protecting the
14 host and the documents in those systems. If you pull
15 together the ideas of redaction that's gone back 50
16 years or more, it's a combination of convergence of
17 redaction and identify of a data element comes
18 together. So it could be for privacy and a number of
19 reasons which brings us down to a whole other line.
20 Working with HSPD-12 and other types of management
21 identity schemes, we're seeing at least in the DOD
22 world of going forward and taking the human identity

1 management and marrying that up with the device
2 identify management; so, the have privileged
3 management. This is basically the intersection of
4 what the device and the data hold in terms of content
5 and identity and what does the person have authority
6 to see and bringing those two together; then we can
7 better match that data and find out if we match up or
8 not; if we do match up, we must find the sources and
9 duration correct. For example, we don't want to send
10 troops into battle because we have the wrong weather
11 report. We have to start thinking about that level of
12 the data and the element and the aggregation of the
13 data and the element so critical going forward.

14 Moderator Crane: How can citizens know what
15 Government is doing and saying in a crisis. This is
16 one of the reasons why Government should be present on
17 Web 2.0 because there will be people there saying what
18 Government is saying. If you're not there, someone
19 will fill that vacuum. Often what gets passed around
20 are links to information rather than information
21 itself and then get the links to that information out
22 along with repeating that information in the social

1 network world.

2 Mr. Drapeau: I will just add an anecdote to
3 "being in that space and people will fill the vacuum
4 for you" and I'm sure you are aware about all the
5 social media and the Twitter business going on with
6 the Iran elections; it's been an interesting problem
7 to track; it could be hard to find out who is the
8 authoritative source and who do I trust and who's
9 really authentic in that space. A couple of months
10 ago there was a military coup in Madagascar; there was
11 a rumor on Twitter that the president was hiding in
12 the palace and because the Government was monitoring
13 this and was able to take action immediately, they
14 were able to dispel that rumor immediately in the
15 media in which it surfaces; then there were able to
16 later produce a press release to the AP, many of whom
17 were surprised anything had happened. So the cycles
18 of decision making are getting more complicated. If
19 you're not already in the space, what I call pre-
20 adapted to the situation which may emerge, you will
21 not have time; you will hear about it second hand; you
22 might not have the authority in that space to be able

1 to take any action at all.

2 Moderator Crane: I'd like to follow up from Mark
3 and Dan and that's regarding data exposure and
4 aggregation. The topic we have been discussing is the
5 reliability of Web 2.0 and Dan brought up a good point
6 about data.gov and then Mark brought up a good point
7 about monitoring your Internet presence when the State
8 Department monitored what was being said about it on
9 Twitter. My question would be how does data
10 aggregation and security issues about data aggregation
11 play into the Web 2.0 space as we're putting all this
12 information out online in a similar analogy to
13 concerns about individuals putting personal
14 information on the social media sites very similar to
15 privacy discussions we've had today.

16 Mr. Chenok: Clearly, our adversaries are
17 aggregating data as well. Security concerns, even if
18 you have good security at a platform level and you
19 have good practices on a personal level among your
20 staff, the information that's out there can be put
21 together in new ways and so quickly that's it's often
22 difficult to respond unless you are there; that's

1 where I go back to the point if the Government tries
2 to withdraw or tries to close off, it will never be
3 able to stop these aggregation threats that arise as
4 Earl said in this question. To be able to have both
5 an offensive capability as well as quickly correct
6 information and identify threats and then spread that
7 information across to the people in the Government
8 that need it and there may be advantages to
9 collaboration enclaves where you might have some user
10 password or some other credential based protected zone
11 where you share that information around; but being
12 able to realize the aggregation threat and respond to
13 that by with let's say all the Chief Information
14 Security Officers for every agency or all of the
15 members of a particular intelligence community about a
16 potential intelligence threat cannot be quickly done
17 by quick blocking of social media.

18 Mr. Drapeau: I have a quick question for the
19 audience. How many of you when you're surfing feel
20 that you are protected out there? Very few. Another
21 thing that we're going towards is even now with
22 Blackberry's; digital signature is one way to ensure

1 that we have safety back and forth. If you think
2 about it, it's really turning the corner now from
3 blacklisting to white listing; everything is bad;
4 things that are digitally signed are good; they're
5 white listed and the only things you accept are tagged
6 and are allowed to come through. There has to be some
7 credentialing going back to the site, the company and
8 even the data itself to move forward.

9 Mr. Burns: I'm most interested in not being on
10 your official computer logged into your official
11 account. I'm sure many people have seen people with
12 an iPhone around the office watching people watch a
13 YouTube video that's blocked on the Dell on their desk
14 in all kinds of workarounds; so, all of these things
15 make into the idea that people are putting more and
16 more information about themselves on the Web than ever
17 before and that can compromise them; that can be used
18 in various ways. I think the cat is out of the bag
19 and it's going to be very hard to dial that back no
20 matter how much you clamp down on what people do; to
21 some extent, this is a mental shift that we need to
22 deal with; how do you look at security of Government

1 information employees in that light. At the same
2 time, I think it's very important people are using
3 these tools when they're not at work because I think
4 informal intelligence gathering will happen at those
5 times. The 16 hours a day you're not at work; you're
6 at lunch and you're on your iPhone at your desk and
7 there's situations where that kind of intelligence
8 gathering and aggregate information can be very
9 valuable although it increases the risk but at the
10 same time you have completely new benefits that comes
11 from this kind of usage of social tools.

12 Dr. Fenton: I don't have too much to add on this
13 topic; there are a lot of sensors out there, sensing
14 every thing and everybody than ever before. That
15 information is more readily becoming subject to
16 aggregation. It's a fact of life.

17 Moderator Crane: Great responses for a surprise
18 question. Now, I have more of the canned questions.
19 How much is it that employees are using social
20 technology in their personal lives and their personal
21 lives may compromise security?

22 Mr. Burns: Yes. As the parent of a teenager,

1 let me say I know this is happening and I think
2 managers may know this is happening; they don't know
3 what to do about it; but, they know something's going
4 on.

5 Mr. Chenok: We're stepping into issues of policy
6 and training and all we have right now is the old
7 security training we all get, and I spent 15 years in
8 Government: the security person coming out with the
9 handcuffs and stuff like that telling you what would
10 happen if you did something wrong; but, it's not
11 viewed as something serious. Norms of behavior in a
12 Web 2.0 in the Government are new and different and if
13 we try to address them with the old style security and
14 techniques, we may not get that far. We need to
15 identify practices to get people to take good steps in
16 their personal and professional persona and as they
17 use social networking; that's going to benefit them
18 in using social media sites at work and at home; I was
19 glad that twice as many people had increased the
20 security settings on their personal social media; I'm
21 sure the Government doesn't have a policy on that and
22 I'm sure that most people usually take their machines

1 and raise it although we may be getting better in that
2 all that time. Verifying authenticity, something
3 comes along you don't understand, verifying it could
4 help in several ways.

5 Mr. Drapeau: I'm going to take a different point
6 of view and I'm going to wager that most people in the
7 Government don't know that their employees are doing
8 this. The people on this panel and most of the people
9 in the room are sort of an enlightened bunch; but just
10 speaking from where I sit at National Defense
11 University and not to bag on them; but, I wonder how
12 many members of the print shop or accounting or legal
13 counsel really have a handle on how often the interns
14 are updating their Facebook entries. A lot of that
15 information may be innocuous and as time goes on,
16 things may change; more and more people are doing this
17 kind of thing; it's not so hard to track down who's
18 working in accounting at National Defense University
19 and there may be consequences to that kind of thing
20 and I do think education is a very important part of
21 that. Even once we get to the point where the
22 Government has some kind of policy or strategy for

1 using this stuff and it's very clean what you can do
2 and what you can't do, someone still needs to educate
3 millions of people; that includes contractors that are
4 embedded in the Government and other people who deal
5 with the Government; so, I think this is going to be
6 an interesting discussion in this next year.

7 Dr. Felten: The discussion of external Web sites
8 is in a way you need two personas; you need your
9 colleague's life and a friend's life; your friend is
10 on the personal side and your colleagues on the
11 professional side. We also need to put some
12 parameters around this and while we are recruiting, one
13 thing we have to consider is whether or not we put
14 Jane.Doe@navy.mil or John.Doe@navy, now you leave a
15 good deal of friending going on. It's probably time
16 that we put out the Web 2.0 for social networking as
17 we go forward.

18 Moderator Crane: I think it's important to also
19 bear in mind the opportunities that can come from
20 having your employees out there in social networks in
21 their private lives. In the technology industry,
22 there are really some countries that have done a

1 tremendous job getting good will among their potential
2 customers. Blogs, Twitter and the like users are out
3 there using it and is respected among others for
4 knowing it and actually can help the Department,
5 instead of having none at all. On their blog, just
6 because they're out there doing reasonable things,
7 people will respect them.

8 Mr. Burns: I'll do a little self-promotion.
9 From a security perception, if we put our security
10 professionals, I'll put that hat on; every time
11 there's a new node; every time there's a new task,
12 there's a threat factor. The question is how do you
13 combat that by shutting down and telling people they
14 can't use social networking in their personal or work
15 computers or do you challenge the issues we're all
16 dealing with to come up with new ways to combat those
17 kinds of threats. The idea came up before of using
18 the cloud on work computers which would require a lot
19 of patching; the idea of it is you necessarily have to
20 respond to the increased threat which people do more
21 and more.

22 Moderator Crane: I think this has been a great

1 discussion on social networking and I'd like to
2 discuss cloud computing; so, my first question to the
3 panel on cloud is how would cloud computing increase,
4 help or hinder adoption of Web 2.0?

5 Dr. Burns: Okay; I'll take a stab at that one;
6 fundamentally, we're still going to have to be able to
7 see out through the cloud; there's not going to be the
8 panacea out there that the data centers just go away
9 and we'll have service. Security as a service;
10 software is a service and even the infrastructure is a
11 service; we're still going to have to do either
12 certifications and accreditations or with the new NIST
13 draft document such as 800-39 and 37's and 53a to put
14 those risk mitigation systems in place and understand
15 what the boundaries are, manage them, and that means
16 that we're going to have to change some of our
17 contract language so we put into the hooks of the
18 language that say we will be allowed to put probes in;
19 we will be allowed the SAS 70 audit when we come
20 through the organization. Fundamentally, though,
21 we're also going to need good asset management.
22 Whether it's the Government doing it or whether it's a

1 requirement that we levy on our contractors, we need
2 to know what we have, where it is, who's using it,
3 which has access to it; if we don't know these things,
4 we're not going to be secure. Even though we're
5 shifting, we're going to have to shift smart and we're
6 going to have to roll it out as I've said before, the
7 local weather pattern, versus the national weather
8 pattern; the cloud is going to be national, internal
9 and global and more to the point, for the high ends,
10 that's where we're going to start; for the low ends,
11 we'll need an opportunity to go external with the data
12 that we have; there's a lot of transparency; we can
13 get there; but, we have to manage it appropriately
14 with the service layer.

15 Mr. Chenok: So cloud communication is insecure;
16 but, it can be more secure in some ways with the way
17 we do security. Right now, you've got lots and lots
18 of servers and Web farms and data servers to which
19 have their own manner of interfacing with applications
20 for users for Internet, etc. With the cloud, go back
21 to what Ed said earlier, you've got an immediate
22 instance, a problem; you have risks, not necessarily

1 security risks in the traditional sense because Google
2 and Amazon and other cloud providers would be out of
3 business very fast if their security were not really,
4 really strong; they've got lots of financial services
5 firms subscribing to them and are increasingly working
6 with the Government as well. The issue there is that
7 the data that resides on those servers isn't
8 necessarily in the control of the Government, so that
9 if there is something happens there to the data on the
10 Google server, and there is a security incident, what
11 happens? Is it the Government's responsibility or
12 Google's responsibility? I see it less as a technical
13 issue and more of a security issue. We really don't
14 have it resolved; it's something NIST is looking at in
15 a more foundational area and it's something we'll be
16 hearing more about.

17 Dr. Felten: When you look at all kinds of crazy
18 things happen in a computer server; but, that's okay
19 because you didn't know about it. Now, you take all
20 these crazy things and move them into the data center
21 and there's a huge increase in the number of things
22 going on that you know about; and you can convince

1 yourself that you're less secure than you were before;
2 but, actually, it's an opportunity. My background is
3 as an academic scientist and a researcher. From that
4 point of view, you want to use whatever you want to
5 use, whenever you want to use it to get done what you
6 need to get done. One thing that Linda Wells and I
7 have written about is this idea that in the future, in
8 general and for the Government, we're going to rely
9 less on contracts and more on handshake agreements.
10 What you might call the spontaneous cloud; it's a new
11 thing; I felt like I had to do something. I don't
12 have any answers; I don't know where it's going to go.
13 I understand what Brian is talking about and I know
14 what it's like to work in a Government office; but, I
15 do think we're going to have a lot of situations where
16 people need things that aren't in the official cloud;
17 but, they're in the bigger cloud. This gets back to
18 the point of what people are doing when they're not at
19 work. I think this is a really big problem for
20 managers and employers of security professionals. If
21 people feel like they need some functionality to do
22 their job, there's a good chance they will get that

1 functionality one way or the other; there's not much
2 you can do in a democracy to prevent them from getting
3 at that. I think this relates to what we were talking
4 about earlier in the panel when we were referring to
5 the Millennial Generation. I hate to refer to
6 generations; these guys do this and these guys do
7 that; to a large degree, younger people feel this kind
8 of technology is part of their way of life and they
9 feel they should have it at work. This is the future
10 Government work force and this is certainly a big
11 issue going forward.

12 Mr. Drapeau: Let me just also subdivide this;
13 when we talk about the cloud, there's really three
14 pieces as an infrastructure, which we've primarily
15 been talking about here and a lot of the companies are
16 really up on what travels in data centers in different
17 forms and redundancy and resiliency; there's also a
18 platform as a service, providing the ability to bring
19 things together; that operates as a security through
20 transparency because developers can come together and
21 solve their collective interests to make sure that
22 those platforms and service environments are secure.

1 Software is a service like Google.com and there
2 you're dealing with more application security measures
3 brought into the Web; so, the security level at the
4 cloud has a lot of different levels people are looking
5 at.

6 Mr. Burns: One of the things is we went from
7 glass houses more into the distributive mode: open
8 sources to open sources; we're trying to move into a
9 service level agreement; performance metrics and
10 overseers rather than doers. We are also trying to
11 reduce our greenhouse effect, our carbon footprint;
12 green IT is another silo; but, it really is convergent
13 in cloud computing as to how to reduce the green
14 environment like reducing HVAC; when you virtualize,
15 you reduce the number of threads you have; it's
16 contained in allocation; you've scaled down the
17 threats. Optimization should be the goal there.

18 Moderator Crane: As we migrate sources, how will
19 managing data be different?

20 Mr. Chenok: If you think about software as a
21 service that we talked about, cloud computing is
22 distributing different computing power, it's all about

1 distributing information across a wide range of users;
2 discovering where the computing power is requires a
3 different set of tools to link applications to the
4 infrastructure. This idea of discovery and rapid
5 response I think you'll see more work in the industry
6 that tries to link the application to infrastructure
7 layers as we move out to the edge.

8 Mr. Burns: I would just add to that. In
9 addition to asset management, it is now document
10 management. Content of the data, e-mails systems, e-
11 discovery, e-case management and record schedules all
12 have confidentiality, integrity, and reliability; we
13 must separate recovery from discovery. Getting back
14 to authoritative sources of data, we can build an
15 enterprise strategy. We can look at discovery ad hoc
16 and recovery and leave the IT folks to recover when
17 the thing crashes and allow the OGCs, IGs an ability
18 to discover when they need to without tying up the
19 resources of IT.

20 Moderator Crane: I'd like to thank our panel for
21 their insightful answers to our question; do we have
22 any questions for the panel.

1 Audience participation: How do Web 2.0 tools
2 break security?

3 Mr. Drapeau: One of the biggest risks is that
4 people know where you are and what you're doing
5 constantly if you're doing it right. I think that's a
6 real danger; there does need to be some education and
7 training at the end of the day.

8 Dr. Felten: I think the boundary between work and
9 non-work especially in the social setting means that
10 the restrictions you put on people at work are less
11 effective and are onerous to people; things seem to
12 change and move faster and that's fundamentally a
13 difference.

14 Mr. Chenok: Knowing who you're clicking with and
15 the concept of search engine poisoning and the results
16 of our Google search and if that information leads us
17 to a fraudulent site, that's a problem; the last point
18 is the more the Government searches for information on
19 a commercial site not well schooled as a cloud
20 provider, the vulnerability can lead to new problems
21 that can come into the Government environment.

22 Audience participation: I really appreciate your

1 saying that it's the responsibility of the IT
2 community to develop the infrastructures to adopt a
3 social media; so, I'm curious to know how you view the
4 adoption of communications revolution e-mail as an IT
5 business practice.

6 Mr. Burns: The question is, is e-mail dead? I
7 think very soon we will be moving away from e-mail as
8 the panacea for document management and use of
9 communication for messaging into the Web 2.0 tools to
10 communicate more rapidly.

11 Mr. Drapeau: To some extent, Web 2.0 is very
12 different because they're not just communications
13 tools, they're platforms for consideration and not
14 nearly a one-to-one communications tool; the problem
15 is it's not simple to say you will use this or you
16 won't; there are many vectors of risk and opportunity
17 as well.

18 Mr. Chenok: Industry's really good at being
19 responsive when there's a good requirement with a
20 financial return; having the Government involved in
21 this will incentivize and create innovation platforms
22 and addressing security; I think that will be

1 different channels:

2 Mr. Scanlon: Leo Scanlon, National Archives;
3 Cloud computing poses a challenged like risk
4 acceptance is balancing mission versus value. It's
5 very hard to see how risk acceptance somebody has to
6 buy the risk of what's occurring in an environment you
7 don't control; bridging that gap is a really tough
8 thing and we're barely out of risk/compliance. At the
9 management level in the Federal agency, Web 2.0 seems
10 to be a ready or not thing and my question is how
11 ready are we and how are we going to bridge that gap?

12 Mr. Burns: Is that a rhetorical question?
13 Fundamentally, we're going to look at the contract
14 language and outsource; if we're going to commercial
15 site, most people are thinking a three month not a seven year
16 schedule; we have to build that into our contracts; we
17 have to put the probe into the environments as we go.
18 Your point about where is the value, capitalization
19 has to occur here.

20 Mr. Chenok: In terms of is the Government ready,
21 whenever there's technology that's new, the
22 Government's not ready and neither is industry, so how

1 can we come together to do this more rapidly than in
2 the past; in other words, we could actually tweet on
3 this tonight.

4 Mr. Drapeau: There's is this perception out there
5 that the Government is behind the ball on this and
6 private industry is way ahead doing customer service
7 and so forth; that's bull; there are few examples of
8 companies doing a great job doing this stuff. Usually
9 the success stories are pretty one dimensional like
10 Ford employees may use Twitter very well; but the
11 company's going bankrupt. The examples I see at the
12 Department of Defense are up there with the best of
13 users.

14 Dr. Felten: I don't see a lot of clever planning
15 in strategy broadly across the industry; I think
16 companies are using these because companies have
17 adopted these but some individual has just started
18 using them.

19 Moderator Crane: You have the last question.

20 Mr. Schwartz: Ari Schwartz, Center for
21 Technology. In regard to trust zones and platforms, I
22 wonder what the feeling on how you go about vetting

1 policy for different applications; do you use vetting,
2 like Facebook vetted this; so, it's okay; or do you go
3 to the agency that vetted it and go from there.

4 Mr. Drapeau: the way that we approach policy is
5 still based on the rainbow series and the system
6 centric control; we need to look at data as the
7 resource you're trying to protect and the system as
8 the container; virtualization technology helps to make
9 you more inherently secure. There are a multitude of
10 reasons why virtualization is helpful. All this is a
11 different way of looking at data that is system
12 centric. It's not called system security; it's
13 information security. Usually you have to get burned
14 a few times before you realize you have to look at
15 things differently. I hope it's not any of us who
16 gets burned.

17 Mr. Burns: The environment that the developers
18 come together should be open; it's difficult to
19 restrain developers in these technologies; on the
20 other hand an open source model could give many
21 opportunities; you can't over engineer this approach.

22 Moderator Crane: I want to thank all of you for

1 staying today and I want to thank our panel, very
2 insightful conversation.

3 Closing Remarks:

4 Mr. Kropf: Good Afternoon, I'm John Kropf. I'm
5 the Deputy Chief Privacy Officer for the Department of
6 Homeland Security. I was going to attempt to close
7 out the first day with just a brief recap of what
8 we've heard today. There's been a lot of talk of
9 metaphors and analogies and I really like that; so,
10 I'm going to try to string together everything we've
11 heard in a matter of a moment or two. We heard Vivek
12 Kundra open up this morning with really giving us the
13 charge that we need to do social media while doing
14 privacy and security at the same time. He made a
15 very, what I thought, inspirational reference to
16 Stephen Ambrose' book, Undaunted Courage, detailing
17 the journey of Lewis and Clark and so I'd really like
18 to use that as kind of the theme for what we've heard
19 today. There's this great excitement to use social
20 media and to push out and to explore and to map into
21 uncharted territory. We've assembled a great team
22 here and that's kind of what we heard on the force

1 panel; we heard about all these new frontiers that
2 we've heard about; we've heard about some very
3 interesting applications that DoD is doing, the
4 Department of State, TSA, EPA. We also need to
5 assemble a great team if you're going to push out into
6 these new frontiers. They talked about bringing in
7 the right stakeholders at the beginning. They talked
8 about bringing in your privacy experts and your
9 security experts; so, all of you, really, in this room
10 are part of that core of discovery if we can broaden
11 that metaphor who are bringing in this technology and
12 so this morning we pushed out over the plains and that
13 was the easy part to explore, the flat open areas;
14 but, after lunch, we hit the Rocky Mountains. The
15 Rocky Mountains are really the new challenges for this
16 new media; how do we intersect with privacy; how do we
17 incorporate with privacy; that's one of many peaks
18 that we're going to be encountering and security is
19 also representative of another of these mountains that
20 we have to scale and we have to do it effectively. I
21 would also say; this is a much smaller peak, a
22 foothill; today in the New York Times there was even

1 an article about the proper etiquette of when to use
2 your Blackberry, when to use Twitter in a meeting; so,
3 there are all sorts of mountains and challenges that
4 we have to face and I think really tomorrow you're
5 going to continue to navigate the map; we're going to
6 continue to look for the right course and our job here
7 is to define the right course, to come back with a map
8 for the future explorers and the settlers that are to
9 follow to map this out in the best practice. We'll be
10 seeing that in our panels in the morning; we have a
11 very exciting speaker, Beth Noveck, U.S. Deputy Chief
12 Development Officer speaking about the Open Government
13 Initiative and we'll be having a panel on legal issues
14 and then finally closing with a best practices panel.
15 So, come back energized, ready to do some more
16 exploring and we'll be ready for all of you here
17 tomorrow morning at 8:30. Thank you.

18 (Adjournment, Day One 4:30 p.m.)

19 Workshop continues on Tuesday, June 23, 2009

20

21

22