

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 23, 2009

MODERATORS

MS. ROSALIND KENNEDY, PANEL 4

MS. TOBY MILGROM LEVIN, PANEL 5

1 PANELISTS:

2 MR. LAURENCE BREWER

3 MR. ROBERT COYLE

4 MS. JODI CRAMER

5 MR. ADEN FINE

6 MS. KIRSTEN J. MONCADA

7 MR. PETER SWIRE

8 MR. ALEX TANG

9

10

11

12

13

14

15

16

17

18

19

20

21

22

1 Panel 4: What legal issues are raised by Government
2 2.0?

3 MS. LANDESBURG: We are going to just hold off
4 beginning just a few more minutes to give people a
5 chance to arrive in light of the traffic problems this
6 morning so relax and enjoy yourselves. We are
7 delighted you are here. We will be back to you
8 shortly. Welcome back to day two of our Government
9 2.0 workshop as we journey along this path of
10 understanding the issues and challenges that these are
11 the wonderful, new technologies posed. I am Martha
12 Landesberg, Associate Director for Policy in the
13 Privacy Office. There's a couple of housekeeping
14 points for all of you. We will begin our first panel
15 this morning and we are still awaiting our opening
16 speaker, Beth Noveck and if she is able to arrive this
17 morning, we will probably just pause the panel to
18 allow her speaking. You panelists are welcome to
19 remain right where you are. Just a quick reminder to
20 all: too please silence your cell phones,
21 Blackberry's, all our little toys and machines. We'd
22 appreciate that. We want to also let you know that we

1 will hold the record of this workshop open until July
2 10th so that if any of you have been spurred to submit
3 comments, information that you want the Privacy Office
4 to know, we will most pleased to receive them at the
5 privacyworkshop@dhs.gov, e-mail address that was
6 in the Federal Register Notice. We will post them on
7 our Web site accordingly. Once again, a reminder of
8 the location of the restrooms on this floor, left out
9 the door, all the way around as far as you can go,
10 past the elevators. And, with that, I'll turn the
11 morning over to my colleague, Rosalind Kennedy from
12 panel number three.

13 MODERATOR KENNEDY: Good morning. Can you hear
14 me? Thank you very much for attending this session
15 which will examine the legal issues associated with
16 Government use of social media. We are very lucky to
17 have assembled such a distinguished panel. Our
18 panelists are: Peter Swire, the C. William O'Neill
19 Professor of Law in Moritz College of Law, Ohio State
20 University; Jodi Cramer, an Attorney in the Office of
21 Chief Counsel at FEMA, Bob Coyle, Legal Advisor
22 Ethics, at OGC; Laurence Brewer, the Director

1 of Life Cycle Management Division at NARA, Kirsten
2 Moncada, the Director of Office of the Privacy of
3 Civil Liberties at DOJ; Alex Tang, the Senior Attorney
4 at the OGC at FTC; Aden Fine, a Senior Staff Attorney
5 at ACLU. We have reserved fifteen minutes for
6 questions at the end. Please join me in welcoming
7 Peter Swire.

8 (POWER POINT PRESENTATION)

9 MR. SWIRE: Good morning everybody. I am going
10 to serve two functions this morning. One is to give a
11 very brief four to five minute overview of legal issues
12 in connection with Social Media in Web 2.0. And, then
13 I am going to be the person talking about procurement
14 issues when it comes to Web 2.0. So, on the Senate
15 for American Progress Web site, we did an event at the
16 beginning of June where we rolled out three papers in
17 the area of Web 2.0 issues. Most of my talk, or my
18 first time I talk today is this one: six new media
19 challenges, a legal and policy considerations for
20 Federal use of Web 2.0. The second one of the papers
21 is called: "How to Buy Free Software, Procuring Web
22 2.0 Technology for the Federal Government," and the

1 third one, we are not discussing today, is called, "It's
2 Not the Campaign Any More; How the White House is
3 Using Web 2.0," and that draws, during the transition
4 I was the lawyer for change.gov, and the setup of
5 whitehouse.gov. So, it is all publicly available
6 information that is some observations on sort of how
7 the whitehouse.gov is operating, given some
8 constraints it faces. What I am going to do briefly
9 is outline these legal hurdles and number the other
10 people on the Panel, and dive into these in more
11 detail. The first very appropriately for this group
12 and my own background, I was at OMB working in privacy
13 under President Clinton. There is a series of privacy
14 issues right? So, Web 2.0 technologies often gather
15 information; either PII or almost PII, and many of the
16 people in this room know about the persistent cookie
17 guidance from OMB. And, some of the people in the
18 room have thrown things at me for having being
19 involved in writing the cookie guidance at OMB. But,
20 that was in 2000. That's nine years ago and, an awful
21 lot has happened and, I think most people think there
22 ought to be some updating and there needs to be a

1 process for that. There is some hope that's
2 proceeding. Another issue that was very prominent
3 in the privacy panel, yesterday is that data
4 goes to third-party sites right? So, if you go to
5 Facebook, if you go to YouTube, if you go to lots of
6 the other sites, and there is some Government
7 engagement with that; then a lot of questions come up
8 about what are the data practices at that third-party
9 site. The third-parties are offering services to
10 their private sector, to individuals. They also offer
11 services to Government, and how much they then change
12 the rules because, it's Government. It is something
13 that's the subject of discussion. A very large issue
14 for people deploying these technologies is how to make
15 sure that there is access for people with different
16 sorts of disabilities: hearing impaired, vision
17 impaired, color blind, etc. And, you in the room
18 often have worked with Section 508 of the
19 Rehabilitation Act. And again, one of the
20 key legal issues is: if there is a third-party site
21 operating off the Government premises, not even as a
22 necessary contractor for the Government; how far does

1 Section 508 apply? One observation is that Federal
2 employees all the time use their computer resources at
3 third-party sites without disability requirements.
4 So, if you are sitting at your desk, you know, how
5 many of you have ever, when you are sitting at your
6 desk gone off-site to use a search engine such as;
7 Google or Yahoo, right? Everybody, right? And, there
8 is no legal requirement at that moment that you only
9 go to Web sites that are 508 compliant. So, we already
10 have lots of going off-site without having 508
11 compliance. But, exactly what the lines are there is
12 something that is going to need a lot more
13 clarification going forward. A third issue that is
14 discussed in the paper has to do with commercial
15 endorsement and advertising. I was sort of interested
16 to see the Spam Can up yesterday in one of the
17 pictures, and you know, when you are the Government,
18 you are not to suppose to be picking winners and
19 losers. On the other hand, we live in a world where
20 trademark goods are pervasive, and so how do you work
21 through what counts as an endorsement, what's
22 advertising, what sort of terms of use do you

1 negotiate around that? A fourth issue which we'll get
2 into more detail today is issues around terms of
3 service that two well-known examples, many terms of
4 service from two point of providers say State law
5 shall apply. Well, that's nice except it's
6 unconstitutional as applied to the Federal Government,
7 right? There is a supremacy clause in McCollough v.
8 Maryland. So, you just can't do that. A similar
9 thing is there is also an indemnity provision all the
10 time in these terms of use which says that the Federal
11 Government shall indemnify. The problem is that
12 violates the Anti-Deficiency Act as illegal for
13 Federal employees to agree to, and yet, we do sign
14 onto these in many ways, and now we are trying to
15 regularize it, and figure out what to do in terms of
16 service. A fifth issue that was mentioned yesterday
17 is Paperwork Reduction Act. When you are doing
18 surveys, that could be the sort of a burdensome
19 collection of information from the public, the PRA is
20 supposed to stop. In themes like just doing good
21 analytics, and common sense, and better user activity to
22 read master, so that has to be thought through how

1 that is going to work for 2.0. And, the last one just
2 came up somewhat in the last program yesterday, last
3 panel. Our computer security issues as we work with
4 software; what kind of certifications, if any, do we
5 accept? What kind of rules and limits do we put on
6 the use of these activities by Federal employees? One
7 thing I know is that the press shop, and the
8 communications shops, and a lot of agencies sure think
9 they need to use these techniques to get the message
10 out. So, if you have agency-wide bans on certain
11 applications, the press people go nuts, and just find
12 ways around it, and then just say, you must be
13 kidding. So, the lawyers and the press people, and
14 lots of other people have to talk about that. One
15 issue that was briefly mentioned yesterday that I
16 think would be much bigger going forward is that
17 oftentimes platforms are themselves secure; but, there
18 is lots and lots and lots of applications that plug
19 in, and the security and privacy practices around
20 those are much less understood. So, those are issues
21 I think, we'll see a lot of discussion of going
22 forward. So, with that said, the outline for this

1 legal panel, I will go through procurement. Jodi
2 Cramer is going to do terms of service. This is what
3 I understand. If I am wrong, you guys will correct
4 me. Ethics and endorsement issues will be Bob Coyle.
5 Records management, which is a great big issue, right?
6 We have Federal Government in there, and sort of
7 requirements, Laurence Brewer will discuss. Kirsten
8 Moncada will talk about Privacy Act, and other privacy
9 issues. Alex Tang will go on some set of issues
10 including the ever-popular FACA, the Federal Advisory
11 Committee Act, which says any time you want to get a
12 group of people together to do something useful is
13 probably against the law. So, see I am not in the
14 Government right now so I can say these things. And,
15 then we will have First Amendment issues including
16 some of the bloggings sort of things that Aden Fine
17 will discuss. So, that is the overview on the legal
18 part. Now, I am shifting to me as one of the members
19 of the panel talking about procurement issues. If
20 ever of you are buying this free, or at least you
21 don't have to pay money for it; software services, and
22 I will briefly describe in about two slides the

1 history of Federal procurement of software. Then, I
2 will talk about three big options for thinking about
3 procurement in this space. One, is we can use a
4 formal procurement process with all the safeguards,
5 and all the paperwork that includes. And, at the end
6 of the extreme is we can enable open-use. Say, come
7 on folks, just go do it, stop worrying about these
8 rules. And then, we will have, what I call,
9 conditional use in the paper. And, we have some
10 recommendations. And, all of this part is tracking my
11 paper and procurement that is available at the Center
12 for American Progress Web site. So, a history of
13 software procurement. Way back in the old days,
14 1950's and 1960's, the Federal Government, when it
15 wanted software use often had to write custom
16 software. If you were NASA, and you want rocket ships
17 to go to the moon, it was hard to find at Best Buy,
18 right? And so, you have to find somebody to write
19 your software for you. And, we'd have very detailed
20 specked out contracts for custom software. But, over
21 time, by the time we got to the 1980's, we had a lot
22 of commercial software products. And so, by the time

1 we had Word and Word Perfect, and all sorts of word
2 processors, we didn't want Department of Defense, or
3 somebody else specking out a custom word processing
4 language. We can do a lot better probably. Faster,
5 better, cheaper if DOD bought commercial products or
6 more recently open source products when that was
7 appropriate. So, commercial off-the-shelf, and the
8 use of GSA schedules was familiar to people. A
9 procurement system built up to try to take advantage
10 of economies of scale. The third phase or this phase,
11 the set of questions we are facing has to do with free
12 services. Free, in the sense that there is no Federal
13 dollars going out the door for a lot of these services
14 at the moment you sign up for Facebook, or use YouTube
15 or Twitter, or a lot of these things. Now, under
16 the FAR, the Federal Acquisitions Regulations, under
17 the procurement law that we know and love, that
18 procurement law applies to "the acquiring by contract
19 with appropriated funds." So, the trigger for when you
20 have to do procurement is when you are acquiring by
21 contract with appropriated funds. If it doesn't fit
22 in that definition, then the basic definition of the

1 FAR does not apply, and you are not in procurement
2 land. Now, you could say, well, maybe that is because
3 they ought to pay us, because we are so wonderful and
4 so worthwhile as a Federal site; that it might be what
5 is sometimes is called, a concession. Like, getting
6 the restaurant at a national park that McDonald's and
7 other people would bid for. Concessions, though under
8 the law, typically involve payment of money to the
9 Government. McDonald's pays the Government for the
10 right to have that, and typically Facebook is not
11 paying. Is anybody getting paid by Facebook to run?
12 No? So, that doesn't seem to fit. We don't have
13 dollars going either way. And, so just as this sort
14 of straightforward threshold matter, it's likely not a
15 procurement under the FAR of the Defense Acquisition
16 rules when the agency signs up for these 2.0 free
17 services. Okay? That is first step. Do you have to
18 go through procurement? Well, it doesn't seem to fit.
19 Should we use procurement anyway? There's very
20 important policies underlying our experience with
21 procurement policies. We have well-defined and feared
22 procedures. We have multiple vendors who are able to

1 educate you, educate the Government about all the cool
2 services they do, all the functionality. Also, having
3 a procurement process reduces the risk of favoritism
4 or precedes favoritism. Why did you select this Act
5 instead of that Act? Well, we had a good process.
6 And, another thing that's not discussed enough in the
7 paper, but, is important is, if you do a good process,
8 you can avoid the problems of lock-in. Where on day
9 one, it might be free but, so is that stuff the dealer
10 gave you from something else so, as to even, on day
11 one it's free, but, then over time there's cost of
12 maintaining it, and it is difficult to shift to other
13 services. And so, a procurement process might help us
14 get the best service at the lowest long-term cost of
15 ownership, and those are reasons to have well-defined
16 and good processes when we choose our software. On
17 the other hand, going through a full procurement, will
18 undoubtedly slow the use of Web 2.0 which
19 whitehouse.gov administration is favoring, and is
20 cool, and it does many good things for agencies if we
21 learn through the conference. And, that's especially
22 true for smaller sites, and smaller agencies, and

1 smaller uses where it might be hard to get attention
2 from the procurement people for your relative small
3 project. Also, it is not clear, quite how you do
4 procurement when it is not covered by the FAR. That
5 is something other lawyers who might know more about
6 than I do but, it's not clear you can to procurement,
7 and the procurement rules don't apply. Plus, there is
8 the administrative burden of approving each one of
9 these contracts through the full procurement process,
10 and they don't see this sort of formal procurement in
11 the private sector every time somebody signs up for
12 one of these things. So, why is it with it for the
13 Federal Government agencies to have to go through the
14 hassle? So, full procurement seems like a lot of
15 burden, and maybe not clearly lawful. So, maybe we
16 should go the other way. The other direction is,
17 maybe we should try to have Government agencies and
18 individuals sign up for 2.0, the way private
19 organizations do which is basically, you just sign up
20 for it. The advantage of this is that would encourage
21 rapid adoption of these technologies consistent with
22 the leadership interest in these areas. In encouraged

1 experimentation, right? We are in the early phase of
2 learning how to use these formations, and we want to
3 encourage a lot of people to try a lot of things, and
4 figure out what actually works. A few dollars than
5 paying for software, so we want to encourage having
6 less expensive options, rather than expensive options
7 that go through the procurement process. And, the
8 favoritism concerns are maybe manageable to maybe
9 limited, because there is no actual flow of dollars to
10 the vendor. They are actually providing bandwidth,
11 and so, they are not getting rich in any obvious way
12 at the Government expense, and not in the sort of
13 simplest way to get rich is which I hand you money.
14 On the other hand, this kind of, let a thousand
15 flowers bloom and forget the lawyers' approach. Still
16 has the risk of favoritism and lock-in especially for
17 high visibility sites. If whitehouse.gov picks one
18 provider every time, I promise you that there will be
19 criticism. There has been, even though they haven't
20 done that. And also, open use, and this gets into a
21 lot of the other legal issues we discussed would not,
22 validate would not sort of give full effect to other

1 important Government policies. The dot polices about
2 privacy, about security, about disability access,
3 about FOIA, records issues, and all the rest. So,
4 just sort of saying, go off and do it, and don't talk
5 to the lawyers' risks undermining important public
6 values that are built into law. So that is not
7 entirely an attractive option. So, as with most
8 option papers there is this magical sweet spot, option
9 three, conditional use that tries to give you some of
10 the advantages of the first two options without as
11 much of the disadvantages. So, we see that there is
12 really a sliding scale all the way from formal
13 procurement with all that paperwork, all the way to
14 just sign up for it, and don't tell us what you are
15 doing. And, there is a lot of places in between you
16 can be, and a lot of people here in different agencies
17 or, in different spots on that sliding scale. So, if
18 we are going to put some conditions on adoption of 2.0
19 technology, one approach is you can have procedures in
20 place. You can say, we don't really need to tell you
21 exactly what all the standards are, it's complicated,
22 and it's new but, maybe get general counsels off to

1 say that is good enough. Or maybe get one level of
2 management, or another to sign off, and say, that is
3 good enough. We are basically covering your behind,
4 and this is really okay. That is a way to say that
5 there is sort of, somebody responsible engaged with it
6 when there's decisions made, but we don't have to get
7 too locked down with all the details. Another
8 procedure that I sort of like the idea of, is try to
9 use 2.0 approaches to govern 2.0. So, when you roll
10 out a technology, when you pick one vendor for free, I
11 suggest having a comment section. So, that other
12 vendors can say, wait a second, we can do more
13 function and help you serve your mission better. So,
14 that interested people in the community can say, hey,
15 there's these alternative technologies that do it
16 better. And, you could say to the Web managers, every
17 six months or whatever, they should give us a report
18 on what those comments have been. This gives us some
19 of what procurement gives us which is, there is
20 different supplies out there who are really expert in
21 their own products and services. And, there should be
22 some mechanism for them to educate the Government

1 about the good things they have to offer. And, if it
2 is transparent enough, and if we see there's some
3 clearly better idea, then that puts pressure on the
4 agency to get to the better thing. So, this is just
5 me but, I suggest having that sort of comment section
6 as you are designing your own technologies. You also
7 put conditions that are substantive conditions. So,
8 instead of requiring a hundred percent full compliance
9 from the first moment you touch software, you can say
10 that agencies should consider the various issues.
11 They should have criteria for privacy in 508 and the
12 rest as important criteria in selecting what they go
13 with. That recognizes that we haven't had time to
14 write all the guidance yet, to have OMB perfect
15 answers on all the issues, where the statutory updates
16 on all the issues. But, these are important
17 considerations, and there should be some set of
18 reasons, or at least a process to look at that. And,
19 a major is to teach strategic question. I ask this
20 question yesterday to one of the panelists. How hard
21 do we insist on complete compliance with everyone of
22 our current rules for all these third-party services

1 during this start-up phase? We are still less than a
2 year from many agencies, or either using these things,
3 and on the Net we know when there is new software.
4 They try version one, and get to version two as fast
5 as they can; version three, version four. We heard
6 yesterday that it turns out having parking lots is
7 important when you are getting too many public
8 comments about birth certificates, we heard. So,
9 there is a lot of things you learn as you experiment.
10 And so, I lean on this item a fair bit of
11 experimentation and flexibility in the early phase,
12 recognizing we will get towards regularity as we go.
13 So, this is my last slide, and then the real lawyers
14 who are within the Government can tell you stuff. My
15 paper supports conditional use that is fairly close,
16 that leans in the direction of open-use. I think we
17 are in an experimental phase. I don't think we have
18 all the answers yet. I think we have a lot of
19 questions and issues that this conference and others
20 are spotting. But, we should lean towards trying a
21 lot of these things, and seeing what the problems are.
22 I would support a policy statement from high levels

1 encouraging 2.0, and transparency about how 2.0 is
2 being used. I think we are seeing that whitehouse.gov
3 is a model, if they are doing it, then how bad can it
4 be if we do it? Right? That is an argument you can
5 use in your agencies. I talk about this public
6 comment feature so that we try to get feedback from
7 vendors and the public, in the online communities.
8 And, I suggest that we consider having privacy, 508,
9 and all these other legal issues from our Panel as
10 explicit things that managers should be looking at as
11 they do this, but not saying you have to have a
12 hundred percent answer before you know how to even put
13 it up. And, then last point, and this is something I
14 can say that the lawyers and the agencies have a
15 harder time saying. I think it is quite likely we can
16 change some statutes here. Change some regs here.
17 Change some OMB guidance here between now and the next
18 couple of years. And, the way to do that is if the
19 people who are involved in that side of the process
20 know what the problems are. Well, you might be able
21 to turn yourself into a pretzel, and legally comply
22 with today's version. But, it might be better if you

1 could just change a clause in one of these statutes so
2 you don't have to do that. I think there is
3 willingness in Congress. There is willingness in the
4 White House to change the statutes, to take advantage
5 of these new things. And so, I am going to ask you all
6 to start thinking about what those changes can be, and
7 how within your organizations, you can start to
8 surface simple statutory changes that would make your
9 life better, and achieve the mission of your agency
10 better. It is hard for people inside their lanes to
11 tell anybody, this is, we have to change a law. But,
12 it makes sense we have to change some laws here. So,
13 I invite you to help with the process. Thank you.

14 MODERATOR KENNEDY: Thank you very much Peter.
15 Please join me in welcoming Jodi Cramer.

16 (POWER POINT PRESENTATION)

17 MS. CRAMER: Hi everybody. I am glad to be back.
18 I am going to talk about third-party agreements, and
19 some endorsements issues. I actually negotiated the
20 first Federal Government agreement with Gulf for
21 YouTube back in the Fall of '07, Spring of '08. And,
22 I am going to tell you what we went through because,

1 we had a hard time. It took us about six months to
2 negotiate the first YouTube agreement. This was
3 before GSA got involved. They didn't get involved
4 until after the election. And, we were on our own.
5 So, it was kind of fun. And, just for those of you
6 who think it's really easy to get the company to
7 change something, it's not. They are a private
8 entity. They have their business strategy, and a
9 couple of them told us, they weren't sure if they
10 wanted us on their site. In fact, Flickr, we had a
11 conversation with Flickr around Thanksgiving of '08
12 right after the election. And, we were all ready to
13 talk to them about changing the agreement and, they
14 basically said to us, well, not all of our people are
15 in the United States, and we are not sure if we want
16 you as part of our community. And, they never got
17 back to us. Despite the fact we called and called and
18 called. So, you know, we are trying to come to them
19 to use their product. They are not coming to us. So,
20 it's not as easy for the Government to mandate what
21 they want in these agreements. So, we can't always do
22 that. This is not the easiest thing. We have certain

1 things we have to change legally. So, that becomes
2 our priority. Anything else is just icing on the
3 cake, if we can get it. And, most of the time we
4 can't. It's a hard enough time to get some of the
5 changes made, and I am still struggling with a couple.
6 So, as Peter talked about, the first issue is: is it
7 a license, a contract, or a gift? And, most social
8 media agreements, we determined are licenses.
9 Because, their parts give the users free of charge
10 over an evocable will, and they are not contracts
11 governed by the FAR. And, if user appropriated funds
12 as Peter mentioned, you have to go through the FAR.
13 But, sometimes you can accept them as a gift, if your
14 agency has gift acceptance authority. And, not all of
15 you do. We happen to but, we are special. And, you
16 cannot accept a gift if you, you can't solicit a gift.
17 So, they have to come to you and offer it. So, if
18 Flickr comes to you, and offers you their premier
19 account, you might be able to accept it under your
20 gift acceptance authority, but you can't go to them
21 and ask them for it. No - - And, Bob will talk about
22 that more. He is the expert on gifts. So, in the

1 terms of service themselves, there are several problem
2 causes, and these are common in most terms of service.
3 Twitter, for some reason doesn't have these issues.
4 But, YouTube does; Flickr does, Ning does; WordPress,
5 Blogger; Advis, all the others do. And, the first one
6 is changes to the terms of service. Indemnification,
7 confidentiality, choices of laws, and then using the
8 agency name or seal for marketing purposes. So, most
9 terms of service agreements, if you start to read it,
10 where you do your click-through which is when they
11 said, you want to sign up, you click yes, and you
12 accept the terms which most of us don't read. It says
13 the company made changes to the Agreement by posting
14 them on their Web site without notifying you. This was
15 a Facebook issue. Where everyone got upset when
16 Facebook changed the terms of service without telling
17 anyone. And, then all the users got mad, and then
18 they had to change it again. So, having this clause
19 in there defeats the purpose of changing the
20 agreement. Why would you allow a contract to have a
21 clause that said they can change it at will, if you
22 need to make changes? They could just change it back.

1 So, you have to propose a notification period with a
2 time limit for the agency to concur with the proposed
3 changes or terminate the agreement. And, you have to
4 be willing to walk away. It is not legal, we can't
5 find. And, one of the things you have to remember is
6 if you sign without it being approved by your General
7 Counsel's office, you can be held personally liable if
8 anything goes wrong. So, you don't want to do that.
9 Indemnification is the big issue that usually everyone
10 sees. And, that means that the user will compensate
11 the company for any damages to third-parties from the
12 user's activities. They're really open-ended, and
13 they're common. But, we can't have that because it
14 violates appropriations laws. Because, we can't
15 expend money that is not in our appropriation. We
16 get, most of us get appropriations for a fiscal year.
17 So, right now we are in the '09 fiscal year. And,
18 when that money runs up in September, you know how we
19 all try to spend it? And, everyone orders every
20 office supply they possibly can, because we can't
21 spend it come October 1st, '08. It's gone. So,
22 unless you have multi-year funds, you can't sign

1 indemnification clause. But, we can be sued under the
2 Federal Torts Claim Act which allows the Government to
3 be sued for damages within that scope. So, you have
4 to change that license, that agreement to state the
5 Federal Torts Claim Act. And, usually most companies
6 would agree to that, because they realize they are not
7 going to be able to sue the Government anyway due to
8 sovereign immunity. So, this links it to the proper
9 statute. Confidentiality. When you get into the more
10 partnership agreements, though they are the ones they
11 deal with; CNN and those people which we end up
12 changing to when we want to go Government-wide. There
13 is a clause that requires confidentiality. But, you
14 guys are all privacy people. You know about FOIA.
15 What can the Government keep confidential? And, you
16 hear it's classified or anything that falls under the
17 nine exemptions, right? An agreement may fall under
18 Exemption 4. Probably not. So, we probably will have
19 to release it. So, make sure you cite in the
20 agreement that you are going to cite to FOIA, and your
21 regulations, not just 5 U.S.C. § 552(a).
22 Because, your regulations apply on how you

1 do with Exemption 4 and confidential business
2 information. Because, each agency has different regs
3 on how they handle it. So, that can be important,
4 because Exemption 4 cases are, APA cases,
5 Administrative Procedure Act cases, so you have to
6 file your agency's procedures. If you don't, then you
7 are going to be held liable in a court. So, you want
8 to make sure the site to your regs, and you follow the
9 procedures outlined in your regs. They also have
10 agreement that says, you know, the State and laws of
11 State acts. Usually, California. Most of these are,
12 you know, San Francisco, Palo Alto. They are living
13 the good life out there while we freeze, or have
14 humidity. But, the Doctrine of Sovereign Immunity
15 does not subject the Federal Government to State
16 courts. So, you have to change it to any competent
17 Federal court. And, contract claims, if it is a
18 contract claims it is in the Federal Court of Claims.
19 It's a tort claim. It goes to a Federal court. If
20 they want to say, a Federal court in the State of
21 California, we can accept that. You can sue the
22 Government in any state you want to as long as it is a

1 Federal court. So, we're agreeable to say, a Federal
2 court in the State of California. But, make sure
3 Federal law applies, and it is a Federal court.
4 Because, we do not want to give jurisdiction to a
5 State court. Because, then we could get dragged into
6 every child support case, and wage garnishment case,
7 and any time the States gets mad, they can take us
8 into their own forum. And, then what is the point of
9 being the Federal Government if that happens? Our
10 benefit is that we won't have to deal with those
11 people, right? So, the other issue which is, Bob is
12 going to talk about in more detail is the use of the
13 agency's name and seal for commercial purposes. And,
14 I know I touched on that bit yesterday about being the
15 seal police, to preventing people from using our
16 trademarks and our seals. But, a lot of these
17 companies want to say, and add this when they sign
18 their agreement with GSA issued to press release that
19 said, these agencies are currently using, add this.
20 So, we went out and market the fact. Now, you know,
21 actually it's a fact, so you really can't go after
22 them for stating a fact. But, it does imply

1 endorsement. So, we usually change the language to
2 say, the company may use the agency's name and seal
3 only to state it's a service user which is a fact.
4 But, as a state that they may not represent or imply,
5 the Government endorses the product, because the
6 Government cannot endorse commercial products. That
7 is a big rule. We have to act impartial. We have to
8 act fair. And, we have to treat everyone equally.
9 So, we can't say we prefer Google over Yahoo. Or, we
10 prefer, you know, MSN over AOL. They are all equal.
11 And, one of the best advices of impartiality is if you
12 are going to start a Facebook page, mark your MySpace
13 at the same time. Because, then you can't be accused
14 of favoritism because you went to both. And, that
15 kind of gets you around some of those obstacles. So,
16 endorsements in the third-party agreement in selecting
17 a service, links to commercial sites, and the use of
18 third-party graphics or trademarks. I talked about in
19 third-party agreements, then selecting a service as I
20 just mentioned, you have to be impartial in all
21 factions. And, you can't give preferential treatment.
22 So, like I said, go to both sites. That solves your

1 problem. And, our philosophy at FEMA is that if it is
2 something that we want our on our network, we are
3 going to build it. It might cost more, but then we
4 can control the privacy. We can control the security,
5 and we are not acting impartially. By building it
6 ourselves, we get around that. And, that's if we,
7 actually one of the best things we could do as the
8 Government is join together to build some of these
9 tools for our own Web site, because that would reduce
10 costs, and get us around all these issues. So, that
11 is something to think about. Links to commercial
12 sites, and Bob is going to talk about this more. We
13 have a policy at FEMA that unless there is a mission-
14 critical need, agencies should avoid linking the
15 third-party sites. Now, we do link to some third-
16 party sites on our site. For example, one of our
17 programs is a National Flood Insurance program. And,
18 we work with flood insurance companies, with insurance
19 companies that sell flood insurance. It's a program
20 we have to run. So, we have to link to those
21 companies, or else we can't run the program. That
22 makes it mission-critical. But, you have to take a

1 look at what is your business reason for linking to
2 that site. Is it just because it's cool? Or, do you
3 have a mission purpose to do that? And, if you do
4 link, they should be accompanied by a bumper or
5 disclaimer. Don't just link. Because, then it does
6 imply endorsement. Also, sometimes when you add
7 contents to your Web site, you get those little
8 graphics and trademarks. And, you should really avoid
9 that unless there is a mission-critical need to do
10 that, because again, that implies endorsements. And,
11 it really doesn't look good for a .gov site to have
12 advertisements from Yahoo and Google, and Digg this, and
13 Techno Karate, and all those lined up on the side or
14 whatever underneath the blog postings. It kind of
15 makes it look like, why is the Government picking
16 these sites and not others? So, you have to be
17 careful. And, with that, I am turning it over to Bob
18 to explain more.

19 MODERATOR KENNEDY: Thank you very much Jodi.
20 Bob?

21 MR. COYLE: Good morning everyone. I can't say
22 that I was dragged into this presentation, but as

1 you've heard from the first two speakers, concerns
2 that are rooted in ethics are kind of in all the
3 topics that we talk about. They get represented in
4 different ways, at different times. Sometimes, there
5 are specific applications of other rules like the
6 procurement rules. But, ethics underlies everything
7 that the Government tries to do. These things of not
8 endorsing, they are founded in the fundamental
9 principles of the Government. The Government tries to
10 do things equally according to the determinations that
11 are logically based on the fact. When we are giving
12 away something valuable, we don't give it away. We
13 have to sell it. That is what procurement is all
14 about. We then give it open competition, so that
15 everybody who is interested in getting that benefit
16 can compete for it. So, underlying all this is
17 ethics. And, whether ethics is the thing that gives
18 you the answer or, simply is the question that needs
19 to be asked is really the issue. And, as Peter said,
20 I think the fundamental problem that is confronting us
21 in the social networking, is that we are dealing with
22 new stuff. We are dealing with a new concept, a new

1 way to deal, and it is a question of, do the old rules
2 apply, or how do they apply, or should they be
3 tailored? Now, ethics is a statement, even those that
4 are specifically and forceful against Government
5 employees, they are essentially a standard by which we
6 measure our performance. And so, when we come to a
7 new, I guess the current word is paradigm; we are
8 coming to a new way of doing business, a new way of
9 going at a question. Sometimes, simply applying the
10 old, the rule in the old way. Taking the rule, using
11 the examples that are in the published regulations
12 don't quite fit. And, I do agree with Peter that this
13 may be one of the things that we are facing here.
14 Let's look at what the rules are. And, it is
15 important to remember that the rules are focused on
16 both individual employees, and on the Government. Now
17 of course, the Government acts through its individual
18 employees, but employees acting in the name of the
19 Government, carrying their title, their position, and
20 representing the Government. So, you have 1) the
21 Government's actions, and then the actions of
22 individual Government employees that are intended not

1 to be the Government's actions. They are intended to
2 be their own individual actions. And so, we get the
3 responsibility of the individual, and the agency to
4 make the distinction between what an employee may do
5 that carries along with it, officialness, and what
6 they are suppose to do in their individual capacity.
7 The official capacity, restriction is essentially the
8 endorsement restriction. It is using your official
9 position in such a way that you create the impression
10 you are read as, you are seen as, picking this one
11 company, this one person, this one service, out of all
12 the other services, and saying, there is something
13 better about this one, there is something the
14 Government likes about this one. This is one the
15 Government says, you should use. The mere fact that
16 that is what you do isn't necessarily bad. Some
17 agencies had specific statutory authority to promote
18 products. So, you have to look and see where your
19 agency is. You have to look and see what it is you
20 are doing. Now, in the context of social networking,
21 I think that's a very important question, and perhaps
22 it's important to me just because I am not familiar

1 with how social networking works. I don't use it. I
2 am not in it on a daily basis. But, it seems to me a
3 lot of these questions first, are addressed by who is
4 doing what. There are agencies that need to use the
5 social networking as a means of getting their message
6 out. I will have a number of examples of agencies who
7 have done that. The Swine Flu, getting out
8 information by the Food and Drug and CDC. FEMA has
9 used those kinds of things for getting information out
10 to the local community, that impact on disasters. So,
11 that is one thing. When the Government is actually
12 going out, and using these things. What does that
13 mean when we do that? That is the clearest example of
14 not putting your message out, or making your message
15 available only on a single channel. We need to give
16 it to other, whatever you want to call them; channels,
17 vehicles, services, that can accomplish the same
18 purpose. Get it out on the various competing
19 services. And, that is relatively simple to control.
20 That is what the agencies are in a good position to
21 do. They can say what they want to do. They can tell
22 who would be the one that pushes the button. They

1 would be the one who says, this is the content we are
2 going to put out there. That's the place where
3 maximum Government control is both appropriate, and
4 it's easiest to do. What applies to individual
5 employees are the things about misusing. Government
6 using their title, their position. Using the
7 Government's equipment services, supplies, their time,
8 for what is essentially personal business. This is
9 not any different than anything else. Just using
10 computers or telephones for personal business. For
11 example, calling home; calling the repair shop to see
12 what the status of the repair on your car is, calling
13 daycare to see about the kids; all those things are
14 examples of things that are clearly the personal
15 business of the employee. And, over time have
16 represented significant discussion points as to,
17 should we be allowing our employees to do that? Now,
18 we have balanced that over time to allow employees to
19 do where there are such things as no incremental
20 costs. You are not bearing a long distance charge to
21 the Government. We have said that that's all to make
22 a few calls on your lunch hour, or your break time,

1 because the employee needs to do things just in order
2 to be productive at work. If you are worrying about
3 things, or taking a lot of time to leave the worksite,
4 go out to a pay phone to do these things, it takes
5 more time. So, over time we have said, these are
6 appropriate things to do with Government resources
7 even though it is personal. Same thing applies when
8 you are talking about social networking. What happens
9 when the Government has the social networking
10 connections available at your desk? What can you use
11 that for that is not Government work? And, you have
12 to look at all the facts. For example, when you are
13 using the Government's name, whether it's your e-mail,
14 or a service that is connected with your employer, you
15 are identified as a .mil, .gov, and so there are
16 certain things that just automatically go with your
17 transmissions that may or may not be appropriate. So,
18 part of these restrictions, these ethics restrictions,
19 are really something that individual employees have to
20 examine themselves when they are doing these things.
21 They have to recognize that where is the Government,
22 the agencies' interest in whatever the message is,

1 whatever the use is they are doing with it, how does
2 it impact, what is the agency's position on the use of
3 this service, this equipment, this time for these
4 purposes? And, I guess that takes me back to the
5 fundamental question is: how do we come to grips with
6 all that? How do we do that? Is that what this
7 conference is about? Is that where we are in time?
8 Where do we balance these things? Jodi has talked
9 about the specific problems where they come up, the
10 linking and things like that. Peter has talked about
11 the procurement side, and what are the terms of the
12 contract. What are we locking ourselves into, what
13 are we doing in terms of blocking other competing
14 services out of. So it's not, ethics is kind of
15 written through the fabric of this. It is not a
16 particular discreet issue, and it's not something, at
17 least in my opinion, we have specific answers to.
18 Because, I do think it is a sliding scale that depends
19 on what the purpose is, what is being done, what the
20 impressions are, that are being created. How is the
21 site read? One of the things that I am ignorant of is
22 how people see a communication on Facebook or all

1 these things. What does it tell the user? Is it
2 saying something more than the individual whose name
3 is signed on it? Or, does it carry with it any of
4 these other aspects. For example, if they are using
5 their Government, you know kind of those kinds of
6 things. Who cares? Was that something that really
7 creates an impression that the Government is behind
8 that? Or, does it vary with the message that the
9 individual is putting on the Facebook? So, that's
10 what I'd like to say about this. I understand that I
11 haven't been very prescriptive as to where we are
12 supposed to be going, or what you are supposed to be
13 doing. But, perhaps we have some questions, some time
14 for questions where I can get into some of your
15 specific questions.

16 MODERATOR KENNEDY: Now, I will turn it over to
17 Laurence Brewer from NARA.

18 MR. BREWER: Thanks Rosa. I just want to thank
19 Rosalind and DHS for the invite. I'm not sure how I
20 got here as a Records Manager on this panel with all
21 these distinguished attorneys. But, I look forward to
22 talking about records management with you, and

1 answering any questions you might have. And, like Bob
2 I am not going to be overly prescriptive, but
3 hopefully we will give you some things to take back
4 with you to the office. Things to think about and to
5 talk to, maybe your agency Records Managers and your
6 staff. So, before I start, I wanted to, get this out
7 of the way first, a little bit of a poll. Who in the
8 audience is a Records Manager or has oversight of
9 records management? Okay, that's like, what four
10 hands maybe? That was optimistic. What about GC
11 staff, attorneys? Okay, a lot more of those. Okay,
12 so for everybody else in the audience, here's a
13 scenario that I've always been curious about. It's
14 4:00, Friday afternoon. You're packing up you're
15 ready to go home. Which visit do you fear the most?
16 A visit from your agency Records Officer, or your
17 General Counsel? Records Officers? Counsel? Oh wow,
18 look at that. Sorry, guys. Well, that's good,
19 because what I am going to talk to you about records
20 management are a lot of the things that I think agency
21 staff have to sit through and endure, and really, you
22 know, I am sure they're thinking how can I get through

1 this? I can get back to my real job. But, I know I
2 only have fifteen minutes. I don't know if you have
3 the hook, but if I go over, please kick me. I have my
4 remarks divided up into four sections, framed by a
5 question. The first is, if this is Web 2.0, why are
6 we talking about records? Second is, this is just too
7 crazy. Can I just pretend this isn't happening?
8 Third part is, is there any help out there? And then,
9 the last thing is just very quickly, what should I do
10 when I get back to the office? So, the first part,
11 usually where we start when we talk about records is,
12 we got to get people an idea of what a record is.
13 While a lot of you are probably aware that there is a
14 statutory definition, if you want to go back to your
15 office, and look up 44 U.S.C. § 3301, you will find
16 this definition of a Federal record. Records include
17 all books, papers, maps, photographs, machine-readable
18 materials, i.e., records. All other documenting
19 materials regardless of physical form or
20 characteristics made received by an agency of the
21 Government under Federal law, or in connection with
22 the transaction of public business, and preserved or

1 appropriate for preservation, by that agency, or its
2 successor has evidence of organization, functions,
3 policies, decisions, procedures, operations or any
4 other activities of the Government or, because of the
5 informational value of the data contained in those
6 documentary materials. So, it is pretty broad. It's
7 comprehensive. I mean the things that I tried to
8 highlight for you there are, regardless of physical
9 form, so this statute was written a long time in the
10 age of books, papers, maps but, it does cover
11 electronic records, and obviously does cover Web site
12 and Web content. Connection with transaction of
13 public business, so as we were talking before, if you
14 go on Facebook during your lunch hour, and you check
15 in with, you know, actually you're probably doing what
16 I'm doing; you are checking with your fourteen-year-
17 old daughter is doing on Facebook, because you want to
18 make sure that she's not getting in any trouble. That
19 wouldn't be in connection with public business or your
20 job as a Federal official, so it would not be a
21 record. But, if you are in a collaborative community,
22 if you are in a Wiki, and you are working on a policy

1 document, that would be a Web 2.0 record. And, the
2 last name appropriate for preservation gets the sort
3 of thinking that you have to do to determine whether
4 or not this something that really needs to be kept as
5 a record, because it reports what you do when you are
6 in a Federal position. So, I guess taking all that
7 in, I mean you have to think for yourself, and this is
8 what we have to explain to everybody else. Records
9 management: is it a help or is it a hindrance? Or,
10 is it just necessary evil? I won't take a poll on
11 that. I'll let you all think about that one. Okay
12 so, Web 2.0. Welcome to the Wild West. This is the
13 reality. And, you know, we talked to agencies a lot
14 about what they should be doing to try and get a
15 handle of this, because they actually grow faster than
16 we can get control of them. And, I would contend it's
17 not a bad thing. Web 2.0 and the kinds of tools that
18 we are using in our agencies, to reach out, to find
19 customers, to find new kinds of customers is a good
20 thing. So, we have to sort of think about how to push
21 what we need to do as far as our mission of the
22 agencies. And, I understand that this isn't a real

1 focus of the current administration, and the bottom
2 line is, it allows us as agency officials to be more
3 effective in our jobs. Because, we can actually reach
4 more. We can get more done, and we can bring more
5 people into the conversation. But, I'm here to just
6 tell you that there is a dark side to that. And, what
7 I mean by that is while we're out pushing, and
8 communicating, but we're not doing, and what our
9 agencies are, they call me up and my staff up is, it's
10 the record of our Government that may be lost.
11 Because, what people are doing is you are working,
12 you're working, you're working, but you are not
13 capturing. You are not thinking about that part of
14 the definition which is, is there anything here that's
15 appropriate for preservation? Is there anything here
16 that really supports what I do in my Federal position
17 that really needs to be saved? It might be temporary,
18 it might just be needed for a short period of time,
19 but there may be significant cooperative projects,
20 e.g. that do need to be preserved for a very long
21 time, and there are a lot of technological issues that
22 we need to think about while working in those kinds of

1 tools for those kinds of records. So, keeping up,
2 there is a lot happening. There is a lot happening,
3 and it's really happening fast. And, keeping up is
4 difficult because of the pace of change. A lot of it
5 we see from agencies where the focus is more on
6 appropriate use policies on talking about user
7 responsibilities, and user roles, and what we're not
8 getting is that drilling down into the records
9 management sphere. So, I mean this is really the
10 challenge, and this is the hard thing about where we
11 are if you have responsibility for records management,
12 or you are working with your records management
13 offices, is if we need to take it down to that next
14 level. Yes, we need appropriate use policies. Yes,
15 we need to know how to tell our users to interact with
16 these tools. But then, we need to figure out how to
17 capture what needs to be captured when we are using
18 those tools. So, what should I know? Just four
19 points that I just wanted to bring up. Things that I
20 was thinking about as I was making these notes. The
21 traditional practices of how we done records
22 management in the past don't apply any more. A lot of

1 which you will see in 36 C.F.R. in the National
2 Archives regulations are really a paper paradigm.
3 Their legacy guidance from a time that did not even
4 envision a Web 2.0 collaborative world. It still
5 works, and we just revised our regulations which
6 should be coming out probably in the next month. So,
7 we will have new records management regulations and
8 hope they reflect more of this world. But, we need to
9 get out of that old mind-set of determining record
10 contents based on that old paradigm. And, one of the
11 things that we need to be more familiar with is; we've
12 been working in these collaborative environments. It
13 just goes without saying but, they engender a
14 diffusion of responsibility. We're all working
15 together, but no one's taking responsibility for the
16 capture, and the information that we're creating in
17 the wikis, and the blogs, and the portals that we're
18 setting up. And, that is really something that we
19 really need. Think about, talk to our records
20 officers, and make sure that they're aware that we
21 need to take some ownership of that. The feud thing
22 is there are new players. There are new roles. We

1 have people like content authors, content owners,
2 content moderators, and these are all specific roles
3 with responsibilities that we never had to deal with
4 before. So, there is probably some record management
5 concerns and considerations that we need to think
6 about around that. And we finally, considering the
7 value of the information, what's appropriate for
8 preservation? From the National Archives perspective,
9 we don't presume that all Web sites, and all records
10 and information that are captured in those Web sites
11 are going to be permanent, and come to the National
12 Archives. We understand that a lot of it is just
13 working papers, kinds of things they're working
14 Web sites that may need to be around for a short period
15 of time to support our business, but then can go away.
16 But, we need to engage our staff back in our agencies
17 to try and figure out what is the value with all the
18 information that we are working on in the Web 2.0
19 world. So, that's a lot to think about. But, there
20 is some help. We have four pieces of guidance, some
21 resources up on our Web site. If you just go back to,
22 when you get back to the office, our Web site which is

1 archives.gov, and then we'll have a link for records
2 managers. And, on the main records management page,
3 you'll find guidance, and there's four pieces and I'll
4 just outline them very quickly in the chronological
5 order. Back in 2004, the first piece came out which
6 was transfer requirements for permanent Web contents.
7 So, for Web sites that were going to come to the
8 National Archives forever and ever, we wrote a
9 guidance document that talks about what metadata with
10 the descriptive information would be needed in terms,
11 so you could capture that and preserve it. So, it's a
12 good thing to have, you know, in the mind, if your
13 working on a project or a collaborative tool where you
14 know the information and it needs to be preserved for
15 a long period of time. Because, it will tell you the
16 kinds of standards in terms of metadata that you would
17 need to have to make that happen. A year later in
18 2005, we came out with our Web management guidance,
19 which is a very broad, general guidance for all
20 agencies on how to manage Web content records,
21 including how to write records schedules forum. And,
22 there are some models in there. There is actually

1 four different models on how you would schedule Web
2 records, and a lot of that might be relevant to the
3 Web 2.0 world. The third piece, as September, 2000,
4 and this is a really good document that I want to
5 encourage to look at. It's called, Implications of
6 Recent Web Technologies on NARA's Web guidance. And,
7 this document is very brief. It's an FAQ. It talks
8 specifically about wikis, blogs, RSS, and portals, and
9 the records management implications of managing all of
10 those, and their agencies and making sure that you
11 address the records management implications for each
12 of those four tools. And then, we have a fourth piece
13 which is actually not out yet; but should be out in
14 the next week or two, and July the latest. And, it is
15 a bulletin that's going to be coming out on managing
16 records and multi-agency environments. So, here we
17 are talking about wikis and what this piece does is
18 talk about some of the ownership issues, if you have
19 many agencies working together in a wiki, who has the
20 responsibility, who should take responsibility, how
21 should those records be captured, and what are the
22 other things in terms of management that we would need

1 to know. So, I would encourage you to go
2 archives.gov. Take a look at those, and if you have
3 any questions, there are seats on phone numbers and
4 e-mails that you can contact that on each of these
5 pieces of guidance. And, then the last thing that I
6 wanted to talk about, alright, what should you do
7 today when you go back to the office? What should you
8 do? One, I think we should think about addressing the
9 diffusion of responsibility, and really start to take
10 ownership, if you are working in any of these Web 2.0,
11 Government 2.0 tools, and we all are. What I would
12 encourage you to do is find out who your agency
13 Records Officer is. If you work in an agency, you
14 have a Records Officer, and they should be aware of
15 the kinds of issues, and they can help point you to
16 the right kinds of guidance. And, if you are lucky,
17 they have contract staff, or a large staff, and I say
18 if you are lucky, that can help you with some
19 guidance, and help you address some of these things.
20 Because, the last thing you want to do is have to deal
21 with these kinds of concerns on the back-end after
22 you've set up a wiki. Or, after you've set up a

1 portal. The time to do these things is on the front-
2 end. When you're first planning, when you're really
3 getting into it before you've really created a whole
4 lot of records, and then at the end you got to figure
5 out, oh, what do I do now? Second, you get into
6 discussions today with your legal staff, your Records
7 Managers, and your IT Web staff. Really, you can't
8 get anything done at agencies without partnerships
9 today. And, you need to really reach out to those,
10 specifically those three communities, if you are in a
11 Government 2.0, Web 2.0 world. They each bring things
12 to the table. They each have things that can help you
13 make sure that the information of your agency is
14 appropriately captured. The third thing is I would
15 say you need to look very closely at the business
16 processes where those particular Web 2.0 records are
17 being created. It is very important that you find the
18 contacts for the wiki, or the blog or whatever it is
19 that you are working with. The business itself will
20 define the value of the information, so when you are
21 trying to figure out what's appropriate for
22 preservation, the only way you can figure that out is

1 within the context of the business process that you're
2 working. So, that is a very critical piece of what
3 you would want to look at first. And, then finally, I
4 would just suggest if you have any questions, if you
5 go through those, there is a person on my staff who is
6 a liaison to each of your agencies who can answer some
7 of these questions, and point you in the right
8 direction. So, I would encourage you to take
9 advantage of the knowledge and expertise of the
10 National Archives help you get further along the way.
11 That's it.

12 MODERATOR KENNEDY: Thank you very much Laurence.
13 Now, please welcome Kirsten Moncada.

14 MS. MONCADA: Good morning. I have been asked to
15 speak to you this morning about the Privacy Act
16 implications of Web 2.0 technologies. And, I have to
17 say I smiled a little bit when Peter spoke about
18 changing laws. Because, the Privacy Act was enacted
19 in 1974, and throughout the twenty years that I've
20 been working on Privacy Act issues, there have been, I
21 can't count the number of times that people have said,
22 oh, this part of the Privacy Act needs to be changed.

1 Or, that part of the Privacy Act needs to be changed.
2 Or certainly, the authors never thought about this
3 technology. The irony being, of course, that in 1974,
4 one of the impetus motivating factors for the Privacy
5 Act was electronic technologies. I can assure you
6 that the authors had no idea that here now in 2009,
7 we'd be trying to apply the Privacy Act to YouTube,
8 Facebook, all these different technologies that are
9 out there. That said, it certainly been a field that
10 keeps us all gainfully employed trying to apply this
11 statute that was really written in a paper environment
12 technologies. And actually, I can say that there is
13 some, even OMB guidance that was written way
14 back in 1975, and the statute itself actually does
15 lend itself to help us interpret. How to apply the
16 Privacy Act to Web 2.0 technologies. And, I guess
17 what everyone knows up front about Web 2.0
18 technologies is, I mean I remember the first time I
19 heard it, I thought it was a thing. And, I was so
20 proud of myself when I said to a co-worker who was
21 more technologically savvy than I: sounds to me like
22 it is just the Internet, and they said, it is. Look.

1 And, they handed me a paper that they had been doing
2 some research. It was just used to the Internet, so
3 we're going to call it something different. And, I
4 think, I mentioned that because of the scope of Web
5 3.0 technologies. There are wide variety of things
6 out there. And, they are only going to keep
7 increasing. And, there is not a fix-all answer which
8 I think the other speakers have mentioned as well. I
9 would love to be able to get up here and tell you,
10 here is the legal answer. It's not going to be that
11 simple. But, what we can do is give you an analytical
12 framework to help resolve Privacy Act issues that may
13 arise in the use of Web 2.0 technologies. And, in
14 looking at this for purposes of our own agency, we
15 will start like we always do with the Privacy Act,
16 with the definition which is often criticized under
17 the Privacy Act of a System of Records. And, much of
18 the Privacy Acts scope and coverage depends on whether
19 or not records are considered to be within a System of
20 Records. And, a System of Records under the Privacy
21 Act is any collection, or grouping of information of
22 records, and let me just footnote though that a record

1 for Privacy Act purposes has to identify an individual
2 and be about that individual. So, it is any group or
3 collection of records that is under the control of an
4 agency from which information is retrieved by the name
5 or some other personal identifier of an individual.
6 Okay. So, one of the key points that in at least
7 applying the Privacy Act to Web 2.0 technologies that
8 we've had to focus on in this definition that
9 honestly, in a lot of other areas, we haven't had to
10 focus on is what does it mean to be under the control
11 of an agency? And that, I think really determine even
12 the threshold question of whether a Privacy Act System
13 of Records is created, when we use certain of these
14 technologies. We really have to look at the level of
15 control the agency has. And, it is easier to view
16 this basically as a spectrum, I think of technologies
17 out there that can basic, and while there will be
18 variance, there is basically three categories. There
19 are Government-owned and Government-controlled
20 technologies which you've heard mentioned this
21 morning. Where we the Government develops a .gov site.
22 Certainly, we can control that. That is, records that

1 are on that Web site, we maintain. They are under our
2 control. We, to the extent, we retrieve information
3 on that site by personal identifier we create Privacy
4 Act Systems of Records. The second model is where we
5 have a privately-owned technology, but it's
6 Government-controlled. So, we use some application,
7 but we basically, we may actually have the application
8 developed privately for our use. This is a fun little
9 part of the Privacy Act that's implicated that most
10 people don't know to much about is a Subsection (m),
11 provision of the Privacy Act. It was basically
12 designed so that agencies could not get out from under
13 the Privacy Act's requirements by having a contractor
14 run their record systems for them. So, to the extent
15 that we control information through terms of service,
16 through agreements regarding the security, to the
17 extent that we put requirements, I mean, we are going
18 to have a whole spectrum here. To the extent, we put
19 requirements on the privacy, security, whatever we
20 want to do. When it starts looking as though we are
21 now controlling it, even though it is being run by a
22 private company, we very well may be bringing that

1 record under the System of Records definition for
2 Privacy Act purposes. The last model is the one that
3 I think is the one, at least with the technologies
4 that my agency is considering that seems to come up
5 the most where we have privately-owned and privately-
6 controlled technologies. And, this is basically your
7 YouTube, your Twitter, your Facebook where the
8 Government uses or creates a presence on those sites.
9 Now, I actually thought your, Jodi's experience was
10 very relevant, because my IT person has been telling
11 me this all along. When we've been probing trying to
12 learn about the technology, and trying to figure out
13 where, who owns, who controls, and let me just say, I
14 know a lot of people that raise their hands were
15 lawyers, you have been hearing this from all of the
16 privacy professionals, organizations for a long time.
17 The importance of the lawyers talking to the IT people
18 never been more important than with this issue. Never
19 been more important. Find someone good in your IT
20 department, and start talking. Really unless you know
21 the facts of how the technology works, it is very hard
22 to apply some of these legal, statutory frameworks.

1 My technology people have been telling me the same
2 thing. They are like first off, even if you want to
3 change those terms of service, they are not going to
4 let you do much. They have absolutely no incentive.
5 I hadn't even heard that they would tell us, no, we
6 don't even want you. We just figure out that, I mean,
7 I have to say, it makes me feel good, because I sit in
8 a lot of these meetings and I think, who wants to go
9 into the Department of Justice's Facebook page? I
10 mean, you know, okay, you see the FBI's ten most
11 wanted, and that's that. You know, what else is there
12 to look at? But, at any rate, you know, there seems
13 to be this notion that, oh, everybody is just going to
14 want to change everything to get us to use their
15 service. So, that experience, the IT people have been
16 telling us all that is not how it's going to play out,
17 and I am pleased to hear that they were right. It's
18 interesting, so to the extent that we are out there
19 using these services, and putting things out there,
20 does not mean they are not Privacy Act implications.
21 Because, they are privately-owned, privately-
22 controlled, and the extent to which we will be able to

1 affect that through terms of service are very limited.
2 We are not creating Privacy Act Systems of Records all
3 over the place out there. However, the Privacy Act
4 implications, and what I would say, is really the
5 heart of the Privacy Act, the Subsection (b)
6 Disclosure Prohibition really bears down here.
7 Because, the way to view those things is instead of
8 receptacles sitting out there, is as a way to push
9 information out of the Government, or pull information
10 in, collected. And, we, I mean, it's interesting
11 because I wasn't sure this is where we were going to
12 end up in the legal analysis. But, in a way, I think
13 it actually forces us to really think of the privacy
14 concerns up front. I fear that if we had come to the
15 conclusion that everything out there on Facebook is a
16 Privacy Act System, I fear that agencies would have
17 been like, okay, well, we've made out system notices,
18 we can post up all over the place now. The
19 interesting affect of the legal analysis is that when
20 you view it as, I am sending this to the Facebook page
21 that DOJ has. It's really no different than, I am
22 sending this to the Washington Post for publication or

1 the Associated Press. The agency needs to be darn
2 sure that if they are disclosing any information that
3 is Privacy Act protected that there is a mechanism, a
4 statutory exception that allows for that disclosure.
5 Works the same way when we collect. If we are pulling
6 information down, and this overlaps completely with
7 the Federal Records Act, if we are pulling information
8 in, and we are using information, we need to make sure
9 that we, especially for using it to take action
10 against an individual, that that record is
11 incorporated into a Privacy Act System of Records. It
12 may be the same thing that lives out there in YouTube
13 land, and out there is not a Privacy Act System, is
14 not Privacy Act covered. But, the minute we take it
15 in, we maintain it, and use it to take some action
16 against an individual we are required under the
17 Privacy Act to give the protection that Act affords to
18 that information. Now, I have no idea what time I
19 started, and as someone told me this morning, you
20 really love the Privacy Act, so I can lose track of
21 time. It is a scary thing. I said I am glad I fake it
22 that well, and Rosalind has known me a long time. So,

1 one thing and I definitely don't want to get into
2 this, because I know you are going to talk about it,
3 Aden. But, the Privacy Act also has a restriction
4 against the maintenance regardless of whether the
5 records are in a system or not, of any record that
6 indicates an individual's exercise of First Amendment
7 Authority. So, take that into account when Aden talks
8 to you about First Amendment issues. The Privacy Act
9 puts you as the Federal agency on the hot seat, if you
10 are maintaining any record describing how an
11 individual exercises his First Amendment activity,
12 unless you have their consent, it's for an authorized
13 law enforcement activity, or there is a statute that
14 authorized you to do to maintain that record. So, the
15 first step, just to, see, I probably rambled right on
16 through this. The first step in this spectrum
17 certainly within, there is going to be technologies,
18 well they look a little bit like they are privately-
19 owned Government-controlled, but I am not sure. I
20 mean one of the things that we've cautioned about is,
21 well, in some respects we need to change terms of
22 service agreements to accommodate us. Realizing the

1 implications that if you do find a new upstart
2 technology provider that says, you know what, we will
3 just be so happy to have your agency. We will do
4 anything you say, realize that if you change the terms
5 of service, such that you are now exercising control,
6 that you very well may bring yourself into creating a
7 Privacy Act System of Records out there that would
8 require notice in the Federal register, etc. So, I
9 guess just to kind of sum up is first I can't
10 emphasize enough, our technology person doesn't know
11 it, but he is getting a call when I get back to the
12 office today. He gets calls from us regularly.
13 Establish a good working relationship with your IT
14 people. Really understand how the technology, and it
15 is a dialogue, because we have, for instance, a
16 component that's dying to use this technology. They
17 are never even really sure how they want to use it.
18 The IT people, having that discussion, we've had
19 numerous meetings just figuring out what exactly do
20 they want to do? And, though we want to do everything
21 just doesn't quite get you there. You have to really
22 drill down to figure out the specifics of what they

1 want to do, how that actually works from an IT
2 perspective, and then apply this legal analysis under
3 the Privacy Act. Are we simply launching a Government
4 site? And, I know our IT people have gone back and
5 forth in terms of, well yes, but if everybody did it,
6 and we all pulled our resources, maybe we could do it,
7 but we don't have budget here so we'll just, it's much
8 better for us to use something that's already out
9 there. I've heard that more than many times as well.
10 So, figure out where you fall. Is this a Government-
11 owned, Government-controlled application? Is this a
12 privately-owned, but let's face it, they are doing it
13 for us. Government-controlled or are we purely in the
14 realm of, this is a private thing out there. It's
15 privately-controlled. We are playing in their field,
16 because there are Privacy Act considerations, but they
17 are certainly different. In the first two instances,
18 you are going to come within the Privacy Act's System
19 of Records definition, most likely. If you are
20 retrieving information by name or personal identity,
21 you will have to publish your Systems of Records
22 Notice. You will have to make sure that the

1 appropriate safeguards, etc. are on that system. If
2 you are out there in pure private sector land, you
3 need to still consider, your privacy concerns are not
4 over. You need to be certain that, just like when you
5 make a press release through Public Affairs, that
6 whatever you are placing on that site is appropriately
7 disclosed. And, whatever you take in, you are giving
8 appropriate notice. The Privacy Act requires that you
9 give people notice when you are collecting
10 information. If your using that as a vehicle to collect
11 things, you need to tell them why you are collecting
12 it, what authority you have to collect it, what you
13 are going to do with it. So, those are all the kinds
14 of things you need to, the analytical framework that
15 you need to work through with these different
16 technologies. And, I am sure as soon as we have
17 applied these to all the ones that are there, there
18 will be twenty more. So, hopefully we will get
19 additional guidance in terms of policy regarding terms
20 of service, and things like that. But, for privacy
21 act perspectives, even though it is an old statute,
22 OMB guidance which talks about that under the control

1 piece of the Systems of Records definition is really
2 what ends up being determinative for us.

3 MODERATOR KENNEDY: Thank you very much Kirsten.
4 Now we will turn it over to Alex Tang.

5 (POWER POINT PRESENTATION)

6 MR. TANG: Hi. Good morning. I am really glad
7 that Kirsten emphasized the control tests. It is a
8 major part of my presentation. I am going to talking
9 about these seven areas in fifteen minutes, and
10 hopefully really get through all of that. One of the
11 areas that I think agencies will have to deal with
12 pretty soon is that people in the public watched our
13 groups, Congress other people are interested in what
14 the Government is doing on Web 2.0. And, we may
15 think, well all of Web 2.0 is public already, so why
16 would they be using the FOIA, why would they be using
17 E-Discovery? But, in fact, Web 2.0 is more than just
18 social networking, of course. It is all this use of
19 collaborative software, creating private spaces where
20 people can deliberate. While that is non-public, a
21 lot of that is exactly where Government business is
22 happening, and people want access to it. So, this

1 charge sort of illustrates three different sets of
2 potential responsibilities. Laurence talked about
3 Federal records. I am going to talk about the
4 definition of agency records which I think is
5 substantially similar under FOIA and the Privacy Act.
6 And then, go on to E-Discovery which is an even
7 broader definition potentially, and creates potential
8 legal and costs. So, let's take a look at the actual
9 definitions. As you will see in that middle column,
10 the FOIA definition has it has been construed by the
11 courts, and includes this control element. And, as
12 Kirsten mentioned, the definition of Privacy Act
13 record or a System of Records includes the notion of
14 control which is also shared by E-Discovery. So, what
15 exactly have the courts said controlling involves?
16 And, this is particularly important with third-party
17 records, that category that Kirsten mentioned, not
18 agency systems or systems created for the agency, but
19 what I will call third-party records. And, the first
20 threshold analysis for control, before you even get to
21 the control tests, the courts have asked; how has the
22 record been created or obtained by the agency? And, I

1 would have to say that I think the word obtain is a
2 little confusing, because you can have constructive
3 controls of something such that you've obtained it.
4 So, let's move directly there. Some courts have said
5 that that's not simply records that you could obtain,
6 i.e. that you don't just have the right to obtain it,
7 but that you actually have obtained it. So, here is
8 the four factors that the courts have looked at, and I
9 think these are things that you are going to have ask
10 yourself with respect to Web 2.0 records. Who is the
11 creator and what was their intent? Did they intend to
12 retain or relinquish control to the agency? What's
13 the agency's ability to use or dispose of the records?
14 Has the agency itself read or relied on the records,
15 and are they integrated into the agency's files, or to
16 the extent they are not? Certainly, in that last
17 element, I think if you were to look at Kirsten's
18 third category, very few, at least currently, social
19 networking sites, is the Government actually going on
20 and pulling down those records, and incorporating them
21 into their files? And, that is again, only one part
22 of the test. And, I will say that as members of the

1 privacy community have discussed whether or not these
2 third-party social networking records or other records
3 created in Web 2.0 are Government records, the common
4 thing I've sometimes heard is, well doesn't the public
5 perceive that they are Government records. And, that
6 can be part of it. I mean, if you are a user on a
7 social networking site, and you post something on a
8 Government's comment page assuming that they let you
9 do so, you might naturally think, well now, it's
10 become a Government record. But, as you can see, it
11 is a multi-factor test. It's not just one thing.
12 And, I just sort of listed a number of factors I think
13 you might think about when we are trying to decide
14 whether or not you are potentially creating record
15 subjects of the FOIA. So, you have to ask first, who
16 created the data or the record? There are a number of
17 players in any sort of Web 2.0 technology and got the
18 agency itself, posting content, maybe creating
19 applications of widgets and posting. Then you've got
20 the user, they may be themselves posting comments or
21 other applications, and you actually have the service
22 providers. They are bundling up information about the

1 users. They've got IP logs; they got buddies' fans or
2 other lists. There is also some other technologies
3 and, this is just a very short list. You have to ask
4 for what purpose was, is that particular activity that
5 the Government is engaged in on the side, or from the
6 user's standpoint? What do they intend with the
7 information that they are posting there? Who
8 maintains the data, and where, who has access rights,
9 and who controls those rights? Again, control may
10 depend on whether you are moderating or not moderating
11 the activity. An important element which has actually
12 come through in the case load with respect to
13 contractors under the FOIA, who holds the copyright or
14 owns the data? I know some of the terms of services
15 either acknowledge the existing right of the service
16 provider to own the data or hold the copyright, and in
17 other cases, it is silent. And, so that is going to
18 be fairly determinative. And, one important point is
19 that with the contractor, it is almost presumed that
20 if you pay them, you own the data. But, in a Web 2.0
21 context, I'd say the payment is not necessarily
22 accessed because there isn't any payment. It is

1 really how the parties themselves define the rights.
2 I mean, as you can see, there is a case that explains
3 that even where the Government paid a contractor, they
4 had especially reserved copyright in their own
5 proprietary software, and it did not become the
6 Government's record. Whoever obtained or disposed of
7 the data, a lot of Web 2.0 services were allowed the
8 user or the account holder to retain or dispose of it
9 at will. In other cases, the service provider will
10 restrict that usage. How and to what extent is the
11 agency user rely upon the data? And, does the agency
12 have the intent to acquire the data for its files?
13 And again, there is some guidance in the case law.
14 The right to acquire the data is not enough. So, even
15 though we can set up an account, and we can control
16 who sees what on a particular social networking
17 account, that may not be necessarily, what makes
18 something an agency record, and that you may or may
19 not have to provide it under the FOIA. On the other
20 hand, planning to take possession may in fact push you
21 over the edge into it both being an agency record
22 under FOIA, and potentially a record for purposes, a

1 Federal Records Act and the Privacy Act to the extent
2 that you are manipulating that data on that site, or
3 through that technology. I would like to move on to
4 what I think is actually an under discussed topic
5 which is the potential for E-Discovery. As we begin
6 using Web 2.0 technologies, weigh against people who
7 are suing the agency or conducting litigation among
8 themselves may see the Government's participation on
9 Web 2.0, and Web 2.0 as a photo place for finding, you
10 know, smoking gun documents. When did the Government
11 notify the class and things like that? And, please
12 note that the scope of E-Discovery is far broader,
13 even if it not a FOIA record, even if it's not a
14 Privacy Act system, even if it's not a Federal record,
15 you may still be required to produce it if you have
16 the legal right to obtain the information. And, that,
17 I think opens up the door to a lot of potential costs
18 and liability. And, unlike the FOIA where you might
19 have a statutory time frame, and can push out those
20 deadlines, the courts are setting the deadlines here,
21 so this is something that I think people have to be
22 sensitive to especially if you are a kind of agency

1 that could be sued a lot. And, the other thing is
2 sanctions. Under FOIA, the basic sanction is, you
3 know, you can be forced to produce the information
4 whereas if you are in a live lawsuit with a party, and
5 you don't produce that information, it can be used
6 against you substantively. The court can conclude
7 that your failure to produce the information and
8 mean something. So, here is some practical
9 considerations. Obviously, you know, at the outset,
10 how likely should I worry about this problem if it is
11 not particularly controversial, and maybe not much.
12 Maybe you do. Do you have mechanisms in place to
13 preserve that information in native format? That's a
14 key element in some cases for E-Discovery is to what
15 extent you preserve all that metadata. And again, I
16 rule to recommend that you not think of Web 2.0 as
17 simply as social networking. Because, it is also a
18 collaborative software. I know, even for the Privacy
19 Committee and the CIO Council, we've created separate
20 spaces where people can share documents. You know,
21 that kind of thing is something that you sort of plan
22 if somebody were to say, I just want all of this stuff

1 that the Government is storing there, that existed on
2 a specific date. How are we going to produce that
3 evidence? Can you suspend disruption and deletion for
4 how long, and who is going to do it? Do you even have
5 control over the person who could suspend deletion?
6 And, why you are maintaining that information, what is
7 the zip, its effect on that system? Is it going to
8 crash the system? How will it affect your on-going
9 business if you have to keep holding this stuff
10 pending resolution of the litigation? Do you have the
11 staffing for this? Who will manage this process
12 including the responsibility or identifying the
13 responsive information? And, of course do you have
14 the funds for that? So, in sum again, I think there
15 are significant responsibilities that you could have,
16 simply by just walking into a Web 2.0 situation, and
17 this is an additional consideration and again, I think
18 people don't necessary think about, they're sort of
19 thinking, purely Federal records Privacy Act. Let's
20 move onto E-Gov. As you all know, Title II has most
21 of the privacy provisions. I think that I really only
22 have time to focus on the two outlined in red, the

1 Privacy Impact Assessments and Web Technologies. I
2 wanted to mention the others as well. I've bulletized
3 one of the provisions. I don't know that if any
4 agency here actually uses provision. Anybody? 35, 44
5 (e). It says that agencies are required to give the
6 public timely notice and opportunities for comment on
7 proposing information security policies. I know that
8 if you look at this language, it doesn't say in the
9 Federal Register, and I gather it's possible, I
10 suppose you could put the Privacy Impact Assessments
11 out for public comment on your Web site to get people's
12 feedback. But, again, a provision that I am not sure
13 to what extent people are paying attention to, but I
14 point it out. Another provision of FISMA which is
15 security related, but I am not sure that it
16 necessarily extends to Web 2.0, at least third-party
17 activities, but something that you should think about
18 is requiring or making sure that you know what is
19 going to happen if the Web 2.0 provider breaches
20 confidentiality of privacy. Do you necessarily want
21 to be participating on a site that doesn't have a
22 breach notification plan? Who gets notified? Will

1 you get notified? And, then Title V, one thing that
2 you should be aware of and again, a provision that I
3 am not sure if everybody is aware of, that if you
4 solicit identifiable information under pledge of
5 confidentiality for statistical purposes, you cannot
6 use that information for other non-statistical
7 purposes. So, let's talk about Privacy Impact
8 Assessments. - - are generally familiar about when
9 you have to do it. I have sort of outlined what I
10 think are some interpretational questions. What needs
11 a PIA and when? The statute doesn't define an
12 information system although there are other
13 definitions that are out there. How does this
14 requirement apply to things that are not IT systems,
15 because I want to be 03-22 which is the memorandum that
16 construes this particular requirement talks about
17 certification, basically talks about events that only
18 occur in a certification and accreditation process,
19 and as a procuring pieces of system software; other
20 things to what extent can or should be applying the
21 certification and accreditation process. I know that
22 DHS, for instance, has privacy threshold analysis to

1 make these determinations. There are agencies
2 building in the PIA process into their change manager,
3 either IT Development. Who is going to do this and
4 how does it apply to a third-party service provider?
5 And again, it is process for a PIA is important when,
6 especially if you are going to be engaged in
7 collecting information. I think it's arguably less
8 important when you are just simply pushing out
9 information, although again, even when you are pushing
10 out information, the service provider may be attaching
11 widgets or applications that could compromise
12 security. And so, this is a good opportunity through
13 the PIA process to address those issues. The second
14 main department that I think we might talk about today
15 is sort of the changing nature of Web tracking
16 technology. I think most people sort of think that
17 OMB's guidance only deals with persistent cookies, but
18 it's phrased more broadly than that, and actually talks
19 about Web beacons and bugs, and those can come up with
20 in third-party advertising of their serve. There are
21 technologies our agencies' consumer ed people wanted
22 to use their technology that could figure out when

1 somebody who received an e-mail opened it up, and that
2 obviously has to use some tracking technologies. And,
3 all of that is subject to the OMB policy, and
4 currently requires agency head approval and compelling
5 need. You have to disclose your use of it on your
6 Web site, privacy policy. And again, if, even if the
7 agency itself is not using this third-party, excuse
8 me, this track and technology itself, to what extent
9 is it being used when you enter into the Web 2.0
10 context? And, obviously, the White House hit this
11 issue with YouTube. Obviously, is looking at this
12 issue, and in the meantime, it was pointed out to me
13 that I believe FEMA has basically created an
14 alternative. If you are scared, or you just don't
15 want to get your users onto a site that can be using
16 this tracking technology, well then create one of your
17 own in post your content there. A few other
18 miscellaneous statutes; Paperwork Reduction sounds
19 like it was previously talked about in a previous
20 session. I think the main issue here is timing, and
21 getting OMB approval, and public comments. You have
22 to sort of build that into your process. You know

1 thinking of technology, such as serving monkey, things
2 that instantly collect, potentially collect
3 information on a wide basis from ten or more persons.
4 Another statute to think about, are you actually
5 managing or controlling an advisory committee? As you
6 can see, that definition of advisory committee is
7 extremely broad. If you trigger this statute, you
8 will have to charter that activity, and put it on an
9 agenda. So, I am really not timed to this to discuss
10 the entire legal definition, but as you can see, again
11 a multi-factor test. But, as we use this technology
12 to solicit comments and bring people together to
13 participate in Government, I think it's more than
14 likely to be triggered. Another statute that is
15 similar, the Sunshine Act which applies to, what I'll
16 call, collegial agencies, boards, commissions, such as
17 the Federal Trade Commission, working has come up,
18 internal blogs, wikis, chat rooms, Second Life,
19 collaborations, software video conferences, all of
20 these providing opportunities for members of our
21 commissions, members of boards to meet in a virtual
22 space. And, when you do that, if they were meeting

1 physically, you would have to announce that to the
2 public, and unless you are having exemptions, you
3 would have to let people attend. So, how do you do
4 that in a Web 2.0 context? And finally, a statute
5 that is very particular to the FTC, because we have to
6 enforce it as the Children's Online Privacy Act and
7 Privacy Protection Act. And again, here's a
8 definition of personal information when you are
9 collecting personal information from children, which
10 is defined as under thirteen, you need verifiable
11 parental consent. And, even if you are not, yourself
12 collecting information, chances are you probably
13 again, social networking, if you are dealing with some
14 of these sites to the extent they don't have age tests
15 or things like that. You should be particularly
16 careful if, before just simply posting yourself on a
17 Web site that might be in violation of COPPA. And, if
18 you go to our Web site, you will see there are some,
19 already FTC approved safe harbor programs, and you can
20 visit some of those programs, and see who are members.
21 And, so those would be trusted sites. And, if you
22 have any questions?

1 MODERATOR KENNEDY: Thank you very much, Alex.

2 Please welcome Aden Fine of the ACLU.

3 MR. FINE: So, I am going to talk about another
4 big issue, and what I see as a potentially very big
5 legal issue for the Government's use of Web 2.0 tools,
6 which is the first thing I'm met. And, as many of you
7 know, the First Amendment makes clear that Government
8 and Government officials cannot restrict or regulate
9 speech except in very limited circumstances. And, it
10 is important to understand the Supreme Court has made
11 clear, the First Amendment law is very well
12 established. And, the Supreme Court has made clear
13 that speech on the Internet is entitled to the same
14 First Amendment protections as all other speech. So,
15 the general rules that everyone is probably somewhat
16 familiar with, with respect to the First Amendment
17 apply to speech on the Internet as well. And so, I am
18 going to focus on a few different areas where I see
19 potential First Amendment issues. First, when
20 Government agencies attempt to control speech on their
21 Web sites, or on their social networking pages, either
22 through moderating the speech, or by prospectively

1 imposing terms of use or restrictions, and what kind
2 of speech users can or can't engage in? Second,
3 briefly touch on First Amendment issues raised. And,
4 we talked earlier, I think Jodi or someone else was
5 talking about links on Web sites. I am going to talk
6 about First Amendment issues raised by having links on
7 Government Web sites. Third, I am going to talk about
8 anonymous speech issues. Finally, and hopefully if
9 I'll have time, I am going to talk about potential
10 First Amendment rights of Federal employees using
11 these sites. So, the first area that I wanted to talk
12 about are attempts to control the type of speech that
13 is occurring on Government Web sites, or Government Web
14 2.0 tools. And, just a kind of a general overview,
15 anytime Government is either moderating speech or
16 imposing prohibitions to eliminate or restrict certain
17 types of speech that the Government doesn't want to
18 occur, that raises serious First Amendment issues.
19 And, it specifically in the Web 2.0 context, or more
20 generally with Government Web sites. There is not a
21 lot of case law directly on point. This is an
22 emerging area, and that is why I think it is a gray

1 issue and a gray thing that we are having this
2 conference where all of you to start thinking about
3 these issues. There is not a lot of case law
4 directing on point. If a court were to consider a
5 restriction on speech in the Web 2.0 context were
6 unconstitutional, the court would likely engage in
7 ordinary public form analysis. And, just very briefly
8 what that means is the court would try to figure, form
9 analysis as generally applied to restrictions on
10 speech that occur on Government property. And, very
11 briefly, the court would probably would want to know,
12 is this a traditional public forum? Is it a limited
13 public forum? Or is it a non-public forum? And, the
14 analysis differs depending on which category you fall
15 into. And very briefly, a traditional public forum
16 are places like, parks and town squares and sidewalks.
17 Places that have historically been places where people
18 congregate and communicate.

19 A limited public forum is a place that's not one
20 of those traditional public forums, but where the
21 Government has nevertheless open office space invited
22 people to come and speak, such as a meeting room in a

1 University. It's not always open to the public to
2 come and speak there and meet there that sometimes
3 Government permits people to do so. And finally, the
4 third category non-public forums. That's generally
5 Government property that hasn't been opened up to the
6 public for speaking purposes, such as a post office.
7 I think an argument, a serious argument could be made
8 that in today's world where people don't really gather
9 in town squares any more, and where people don't
10 really communicate with each other in parks, many
11 cities don't have main streets any more, that in
12 today's world Web sites, Government Web sites, forums
13 created by the Government for people to interact, that
14 those could be called traditional public forums. Now,
15 the Supreme Court will probably not buy that argument.
16 But, it is possible. The Supreme Court has previously
17 indicated that traditional public forums, that the
18 word, traditional is important. That the public
19 forum, in order to be a traditional public forum, it's
20 got to historically have been considered a public
21 forum. That obviously doesn't apply to these new
22 sites. But, I think a serious argument could be made,

1 and one that the courts may have to grapple with.
2 More likely, the court would consider this to be a
3 limited public forum. Where the whole purpose of
4 these sites is to get people to interact with
5 Government, to get people to communicate, to have an
6 open dialogue. So, assuming, and I think it is
7 important also to know that simply putting up language
8 on the site saying, this is not a public forum, will
9 not be dispositive. Lots of private sites, maybe some
10 Government sites do include things like that. It
11 doesn't necessarily hurt, but it's not necessarily
12 help either. So, assuming that this is a limited
13 public forum, the rules that would apply essentially
14 are that restrictions, regulations on speech in order
15 for the Government to justify restrictions, the
16 restriction has to be narrowly tailored to achieve a
17 compelling Governmental interest. But, it can also be
18 time facing manner restrictions put on the speech that
19 occurs on Government sites. However, they need to be
20 content neutral, and they also need to be narrowly
21 tailored, and leave open ample alternatives for
22 communicating. So, that is kind of a general rule.

1 One big difference, and frankly, the rules are
2 somewhat very similar for limited public forums and
3 for traditional public forums. The one big difference
4 is that in limited public forums, you can probably
5 limit the category of speech, the content, if you
6 will, the subject matter to the subject matter for
7 which the limited forum was opened. So, if you have,
8 if you open a message board or blog on, say TSA
9 issues, you can probably limit the speech that occurs
10 there too, TSA related issues. You couldn't speak on
11 school issues, for example. But, other than that, you
12 know, other than the limiting the subject matter of
13 the speech, in general, First Amendment rules apply.
14 In order to for the Government to show that something
15 is narrowly tailored to achieve a compelling
16 Governmental interest that is really hard for the
17 Government to do. That's essentially strict scrutiny.
18 And, most times when Governmental restrictions and
19 regulations falls within strict scrutiny, the
20 regulations is going to be found unconstitutional.
21 So, it is very difficult to overcome that, that tough
22 test. And so, what does this mean for Web 2.0? For

1 Government's use of Web 2.0? I think, it means that
2 there are serious First Amendment problems. If the
3 Government is going to be deciding what kind of on
4 topics speech the Government wants to permit. For
5 example, if the Government is editing comment, an on-
6 topic comments where it's not posting on-topic
7 comments. I think there's going to be real serious
8 First Amendment issues. And, specifically, if
9 Government wants to prohibit certain types of speech,
10 for example, offensive speech, demeaning speech,
11 indecent speech, hate speech, you know, all of those
12 while we may not like those kinds of speech, we may
13 not want that kind of speech to occur on Government
14 Web sites, or on a Government forum. All of those
15 types of speech are protected by the First Amendment
16 and so, just because you don't want them to appear
17 doesn't mean you can legally do so. I think a similar
18 issue is raised, and I think a really big issue; if
19 the policy is simply, we reserve the right to post or
20 not to post whatever comments we want. Lots of
21 private companies can get away with that. The
22 Government, if Government starts doing that, that's a

1 serious issue. The Supreme Court has made clear that
2 Government officials cannot have unbridled discretion
3 to decide what speech can and can't be made. And so,
4 I think in developing these policies and working
5 through these issues, everyone needs to be really
6 conscious of the traditional First Amendment rules
7 permit, and what is not permitted. The bottom line
8 essentially from my perspective at least, and I am
9 sure other people have different views is that once
10 the forum has been opened up the Government can't be
11 deciding whose speech can or can't be made. And, in
12 other words, you got to take the bad with the good,
13 once the forum is opened up. I want to discuss one
14 issue. What I have been talking about is active
15 moderation by the Government itself; By the
16 Government agencies or Government officials. So, a
17 slight twist to this is if the Government Web site
18 gives the power to censor, the power to moderate to
19 users, so it is not the Government that is actually
20 doing the censoring, but it is the users who, a lot of
21 private Web sites have users vote on comments. Either
22 to remove them if they are flagged as inappropriate,

1 or to vote on to determining the importance, the
2 placement of particular comments. Ones that get more
3 votes go to the top of the list; ones that are deemed
4 not to be as valuable go to the bottom of the list.
5 That is not a solution, a constitutional permissible
6 solution either. The Supreme Court has made clearly,
7 called a heckler's' veto which means Government can't
8 let other people, can't let the hecklers suppress
9 speech that they don't like. I think it's a real
10 world example of this. Maybe easier to understand
11 which is if there is a protest occurring outside on
12 the street, I think everyone would agree that you
13 can't let the crowd vote on who gets to protest, who
14 gets to stand at the front of the sidewalk, and who
15 gets to stand at the back. Because, the obvious
16 result will be the majority will prevail. And, the
17 minority viewpoints, unpopular viewpoints, will be
18 suppressed, and the First Amendment does not permit
19 that. And, I think, this, I am not sure what the
20 solution is from Government's perspective I would
21 then, just understanding that you got to take the bad
22 with the good. And that the answer to a speech that

1 we don't like is more speech. And, in the right
2 context, it's actually a pretty good answer. If
3 somebody posts a blog comment that either a member of
4 the public doesn't agree with, or a Government
5 employee doesn't agree with, we can just post a
6 response right away. Have that dialogue right there
7 and then. And, so the answer is not to remove speech,
8 the answer is to counter the speech. The next issue
9 that I want to talk about very briefly are First
10 Amendment issues raised by having links on Web sites.
11 And, whether links on a Web site impacts the First
12 Amendment who really depend on the specifics of each
13 situation. If, a Government Web site permits user to
14 post links, or to add links, for example, to a blog
15 role on the side of the page, then the same exact
16 analysis, the same limited public forum or public
17 forum analysis will apply. In other words, Government
18 can't pick and choose which people or which links
19 Government wants to permit to be posted on the
20 Government site. If, on the other hand, the
21 Government is, the agency is the only one who is
22 deciding what links are put on the page in the first

1 place, that users cannot add links on their own. If
2 the Government retains the sole control sort of the
3 editorial discretion, then it's probably, and I stress
4 probably, it's probably permissible for a Government
5 to decide which links it wants to put on. For
6 example, this is, I'm not sure how this would play out
7 in the real world, but if say, on the HHS Web site,
8 they want to put in a reproductive health category, if
9 Government is the one making the sole decisions in
10 putting the links on, possibly permissible to have
11 simply pro-abortion links, Web sites links. Possibly
12 permissible to have only anti-abortion links. It is
13 going to depend on the circumstances, but once you,
14 again, once you open up the possibility, the forum to
15 allow users to post links or to add links, then you
16 got to take all of that. You can't make distinctions.
17 An exception, I think, and it's a very narrow
18 exception could possibly be with religiously
19 affiliated Web site links. You could run into
20 establishment clause issues. If only a certain
21 religious links are being added to the site. The next
22 area that I wanted to talk about, and I think this is

1 a really big issue, and it overlaps with all of the
2 privacy issues that have been discussed at the
3 conference is anonymous speech. So, the Supreme Court
4 has made clear that the First Amendment protects the
5 right to engage in speech anonymously, and that
6 Government cannot require individuals to disclose
7 their identity to order to engage in speech. And,
8 courts, again in the Internet context, courts have
9 consistently found that this right to engage in
10 anonymous speech applies on the Internet as well.
11 This means that requiring Internet users to provide
12 the personal information in order to speak, or even in
13 order to read material on Government sites, is
14 constitutionally problematic. It's okay if people
15 voluntarily provide personal information, but
16 Government can't require it. And, I think it's really
17 important for all the Web sites to make clear that it's
18 okay for users to provide their personal information
19 for that, we cannot require it. I think the easiest
20 example obviously is requiring somebody's name to be
21 provided in order to post something. But, other
22 information, an e-mail address, telephone number,

1 those also raise problematic issues requiring the use
2 of a pseudonym is probably okay, but again you got to
3 make clear that users understand they don't need to
4 give a real name. I think a really interesting issue
5 is raised if personal information is not necessarily
6 asked for by the Web site. But, if the sites, the
7 agencies are nevertheless collecting and gathering
8 personal identifiable information such as, IP
9 addresses. And, IP addresses arguably are personally
10 identifiable information. They are traceable. And,
11 so collecting IP addresses, speakers poses some real
12 First Amendment issues with respect to the right to
13 engage in anonymous speech. And, I think from there
14 comes the private sector experiences instructive for
15 all of you, you know, companies like Yahoo inside
16 message boards, opening comments sections for years,
17 and something that is likely going to arise when
18 Governments start having open forums, open
19 discussions, is that they are going to be attempts by
20 people to, people postings on the Internet that are
21 sometimes critical. Sometimes, maybe not true. And,
22 inevitably, the targets of that speech want to find

1 out who that poster is. Especially, and this may
2 occur on some of the Government sites, especially if
3 there is a suspicion that the poster is an employee of
4 the company. And so, what's typically happens is that
5 somebody whose, doesn't like the speech will issue a
6 subpoena to the company operating the message board.
7 For example, to Yahoo or to a Government agency
8 operating a Web site asking for information to disclose
9 the identity alleging that, so this poster has, the
10 typical claim is that this poster has engaged in
11 defamation said something that is not true. And,
12 there are issues of subpoenas seeking to obtain
13 information that can be used to identify on the
14 individuals. And, I think with respect to this, in
15 order, there is not a real way to avoid that. There
16 are going to be people who don't like speeches
17 critical of them. But, it is important for the
18 agencies for you all to adopt policies that are as
19 protective of the right to engage in anonymous speech
20 as possible. To limit the logging and the collecting
21 of IP addresses to the bare minimum, to whatever is
22 technically necessary for the site to operate. And,

1 to the extent you do end up receiving any of these
2 subpoenas. It is important to provide notice, and you
3 know who the posters are. It's important to provide
4 notice in their opportunity to challenge the requests
5 to disclose that information before you actually give
6 out that information. So, I am running out of time
7 so, I am not going to have time to go into employees'
8 speech rights, unfortunately. Other than to say, very
9 briefly, that Government employees do have First
10 Amendment rights. The Supreme Court has recently, I
11 think weakened is a good word to use for, the Supreme
12 Court has recently weakened employee speech rights
13 saying, that if a Government employee speaks as an
14 employee, in a capacity as an employee, they have no
15 First Amendment rights. If, on the other hand, you
16 are speaking as a private citizen which Government
17 employees are using social media sites, often will be
18 doing. You possibly have First Amendment rights.
19 However, if private citizen speech by Government
20 employees has a harmful impact on your employer, on
21 the agency, you may not have First Amendment rights.
22 And, the Government's rights may outweigh your

1 individual First Amendment rights. So, the key is,
2 are you speaking as a public employee, or as a private
3 citizen? Second, is your speech harming your
4 employer? If so, you may or may not have First
5 Amendment rights. I think I will just conclude by
6 saying, I think Government's use of Web 2.0
7 technologies is a terrific idea in encouraging
8 increased interaction between the public and
9 Government, it is a great idea. It can be great for
10 the Government. It can also be great for the public,
11 but it's got to be done right. And, it needs to be
12 done in a way that it ensures that First Amendment
13 rights are protected. It would be very ironic and
14 unfortunate. If in an attempt to open up dialogue
15 with the public, we end up infringing on First
16 Amendment rights. Thanks.

17 MODERATOR KENNEDY: I am going to open it up to
18 questions.

19 Q. MS. ALLEN: Hi, I am Sarah Allen. For
20 agencies that have not yet adopted agency-wide social
21 media policies, but who have individuals acting in
22 official capacity on social media sites, I have a

1 couple of questions for this. What are the major
2 concerns and issues, if this is allowed to continue?
3 How should the agency go about trying to fix it, you
4 know in a couple minute answer? And, for the
5 information that is hosted on third-parties, but sits
6 on the Intranet, how do you deal with that as well,
7 for records management and liability, that kind of
8 stuff?

9 A. MS. CRAMER: We, I know we've done is we've
10 incorporated, we do not, we allow our employees to
11 have their own personal sites, and we actually have a
12 memo that we have an on-camera policy which says that,
13 our employees if they are asked by the media to
14 discuss their job, they should talk to the media.
15 Believe it or not, we like to talk to the media
16 because we want them to know what we do. So, they
17 don't bash us as much. But, I would encourage
18 agencies that have people individual accounts we don't
19 allow individual accounts under as an official. We
20 have FEMA wide accounts and for programmatic
21 functions, but I would incorporate those into a
22 programmatic function, like the head of your agency

1 can use the official account. You can have a blog
2 entry from the head of your agency, and that would be
3 like a newsroom type setting which is what we are
4 setting up. You know, there's, if you haven't gone
5 through the new terms of service agreement, and you
6 signed it, you can be held personally liable, if there
7 is any problems. GSA has a whole bunch of new terms
8 of service agreements for certain providers on the
9 content measures Web site. People can use those with a
10 contact number to get those and transfer over, if you
11 don't have legitimate terms of service because you are
12 putting your agency at risk. And, they will help you
13 set up the right accounts.

14 A. MR. SWIRE: One of the, I think I agreed on
15 the legal matter with everything Jodi just said, I
16 have also heard of some senior officials saying, we
17 are not going to hold you liable, we want you to
18 innovate; err on the side of experimenting. We have
19 White House leadership that shows we want to try to do
20 these things. And, so sometimes fairly senior people
21 in agencies are willing to provide protection for
22 people, and give guidance from the top, and one of the

1 things that is hard in all of this is we have various
2 laws. You know, maybe there is some theoretical idea
3 that somebody is going to be held personally
4 responsible for signing up in good faith in Government
5 for an account. I am not aware of anybody getting
6 disciplined for that. Are you?

7 A. MS. CRAMER: You could.

8 A. MR. SWIRE: I'm just asking are you aware of
9 any instances up until now?

10 A. MS. CRAMER: Not to my knowledge, but the
11 best thing to do is really talk to your General
12 Counsel's office, and work with your attorneys. I
13 mean, my Public Affairs person, we sit, we are very
14 close. And, it is better for your agency to talk to
15 the company, and go through GSA, if they are working
16 on it, and get the right agreement. Don't step out of
17 your lane, because even though no one has been
18 disciplined yet, it doesn't mean it won't happen.
19 And, what's the ethics violation? Bob knows the code
20 better than I do.

21 A. MR. COYLE: The ethics violation would not
22 be the problem. I mean, what you are talking about

1 here are all the other things that go along with.

2 A. MS. CRAMER: The unauthorized.

3 A. MR. COYLE: Yes, right.

4 Q. MR. NEWPHEW: Here is Jeremy Newpew from
5 the Interagency Off-site Support Staff. In the
6 Department of Defense, we are very aware of problems
7 with people giving away too much information on the
8 Internet, and how that can convert to huge problems
9 for the organization which I think you just mentioned
10 that there are times when you can create a problem for
11 your organization based on the things you say. On
12 sanctioned or unsanctioned Internet posts. And, the
13 question that I have is, considering that there are
14 inevitably consequences, and possibly severe
15 consequences for the things you post online, what
16 kind of defense do people have if they were not
17 trained in what kind of information they can post, and
18 what they can't?

19 A. MS. CRAMER: Again, anyone who took their
20 new employee ethics training, was trained on not to
21 disclose non-public information. That is one of the
22 basic fourteen principles that is in, what is 5 C.F.R.

1 2635?

2 Q. MR. NEWPHEW: So, if you are an employee of
3 the agency over say, twenty-five years in this thing
4 you read when you started twenty-five years ago, still
5 applies, but you don't know how to apply that to Web
6 technology, you are still held to the same
7 responsibility?

8 A. MS. CRAMER: But, you are supposed, most
9 people of annual ethics training, you are supposed to
10 have annual ethics training, where you get this
11 repeated, and it is not non-disclosing, disclosing
12 non-public information is not something that's special
13 to the Government sector. Martha Stewart, you know
14 was charged with insider trading which is the same
15 equivalent. You know, it's one of those things, if it
16 is not public, you shouldn't put it on the Internet.
17 And that's kind of just a basic principle of being a
18 good citizen.

19 A. MR. SWIRE: Let me, Beth Noveck wasn't able
20 to come this morning, and she is leading the
21 President's transparency initiative which was the
22 first, sorry the second day in office. The President

1 of the United States had this big transparency
2 initiative which says, a lot of the times when
3 Government has leaned against release, we should be
4 leaning for release. And, you know, in some ways they
5 are doing a point, counterpoint on the normal things
6 the Government has had for a long time. When I worked
7 in OMB, my staff and I followed the rule. We could
8 say anything that was true and public. And, if it
9 wasn't, then we couldn't say it. So, following the
10 rules about not releasing non-public is highly
11 important. There is also many problems for Government
12 if we don't release information. There is problems we
13 heard on one of the Panels yesterday that happens if
14 agencies don't get their message out, including for
15 public safety, and a lot of those reasons. And so, of
16 course, you are not supposed to release classified
17 information. You are not supposed to give enemies
18 insights into how to blow up insulations. But, we
19 have a President who has made transparency, including
20 a massive shift in FOIA policy within the first week
21 in the Administration with a President who has gone
22 out and said the presumption FOIA releases are going

1 to be done. It is highly different from FOIA for the
2 last eight years, and the emphasis is on transparency.
3 So, you don't want to release non-public, and you'd
4 certainly don't want to police classified information.
5 But, the President has given extremely clear signals
6 that he at least favors a very big shift in the
7 direction of releasing information.

8 MODERATOR KENNEDY: Okay, we need to take the
9 next question. I'm sorry.

10 Q. AUDIENCE PARTICIPANT: I guess one question
11 on anonymous speech. The interplay between the
12 Computer Fraud and Abuse Act, and pseudonyms with
13 terms of service. Does somebody want to address that?
14 I will just throw it up to the panel because there is
15 potential criminal implications. If you do have a
16 pseudonym registration for an individual, and it
17 violates terms of services which most of these terms
18 of service require you to provide your full name, and
19 other information.

20 A. MR. SWIRE: I'll give it a try. So, I
21 listened to Aden's, you know, very well educated view
22 on these issues. I will say an anonymous speech which

1 is nary I've worked on also that there is precedence
2 that point in a lot of different directions. We don't
3 have an IP address, Supreme Court opinion. Right, and
4 so lawyers, if we ever get one, will be able to write
5 briefs with some different views on that. For
6 instance, when you go to a town hall, it's common that
7 you show your face. And, in many settings, that is
8 going to release your identity. That is going to be
9 more identifiable than IP addressing in many settings.
10 And yet, we don't think that this is somehow violation
11 of anonymous speech that people walk into town halls
12 and show their face. So, there's complicated issues
13 around anonymous speech, and we can imagine the courts
14 having really different view as we get into each
15 specific context.

16 A. MS. CRAMER: And, I think probably the best
17 practice route is basically on blog issues, more than
18 on Facebook or something like that, because we do not
19 control that, but to make, and I know we are going to
20 do this is make anonymous default settings, so that
21 you have to put in a name, but to allow someone to put
22 in no name or anonymous, to give them a right to

1 anonymous speech. And, that way, you are not dealing
2 with pseudonyms; you are not dealing with screenings,
3 but just to give them the right to post anonymously on
4 Government blog. And, I think that would allow for
5 the anonymous speech, and still, you know, not force
6 people into criminal acts.

7 A. MR. TANG: There's a countervailing
8 interest I think though the agency has especially in a
9 public comment setting where we have to know sometimes
10 who that person is who is commenting in order to
11 determine credibility. So, I think our current,
12 public common forum technically allows the option to
13 be anonymous, but I think, that if somebody were to
14 say, well, I submitted you a comment, why didn't you
15 listen to me. If it came in from a regulated entity,
16 obviously we would expect them to identify themselves.
17 If sort of an individual's are commenting in general,
18 I think they would sort of just go into the general
19 pool. So, you know, I think providing that right is
20 one thing, but then when you get to sort of a
21 procedural situation where you have to start weighing
22 the merits of comments, you know, that information is

1 useful to an agency.

2 MODERATOR KENNEDY: One more questions.

3 Q. MS. BARRET: Claire Barrett from TSA. First, I
4 would like to thank you all for an excellent panel.
5 It was really useful for a lot of the issues that I
6 think we are facing inside Government. I have
7 actually two questions, and they are very different.
8 First is for Mr. Fine primarily, I think. But, as
9 agencies consider policies and memorandums governing
10 employee and staff use, personal use, Web 2.0
11 technologies and understand that they are First
12 Amendment issues there. Do you have some guidance as
13 to how those policies might be framed, and then the
14 second question has to do with the use of Web 2.0
15 technologies from a Government perspective, not as a
16 means of communication, so we talked about 2.0
17 basically the public relations forum right? We have a
18 presence in Facebook or a Twitter account or a blog,
19 and we push content out, and we also use it for
20 internal communications, Idea Factory at TSA, those
21 sorts of things. I'm entrusted in your perspectives
22 on using 2.0 and those forms as an intelligence

1 function, so Government collecting information from an
2 open-source perspective of activities engaged. This is
3 really Web content activities. And then, the second
4 part of that is using information that individuals put
5 out there in forum Facebook, Twitter, MySpace, in
6 terms of benefits administration and particularly how
7 that applies to the Privacy Act. So are questions of
8 immigration, individuals seeking asylum or individuals
9 seeking employment, but we see as something contrary
10 to their statements, maybe out on Facebook, to
11 policies and uses. Thank you.

12 A. MR. FINE: So with respect to employee use
13 of social media sites, I think, first the Supreme
14 Court has made clear that where public employees
15 speak, whether it is on the job or off the job is not
16 necessarily dispositive. So, there is no per se rule
17 that anything said on the job, while you are at work
18 means that you are speaking as a public employee. If
19 you are speaking on a matter of public interest,
20 whether it's on the job or off the job, if you are
21 speaking as a private citizen, you have a First
22 Amendment right to speak on those matters of public

1 concern. What constitutes speaking as a private
2 citizen versus in your capacity as a Government employee
3 will be very difficult. The Supreme Courts, it's the
4 Garcetti Decision almost creates a perverse incentive
5 where, if you speak, if you complain about something
6 that is going on to your supervisor, it's not
7 protected. If you complain about what is going on
8 inside the Government agency to the Washington Post,
9 you are speaking as a private citizen. And so, a
10 Government employee going on posting something on
11 Facebook about what's happening on the job is probably
12 speaking as a private citizen. So, you are going to
13 be entitled to First Amendment protections if you are
14 speaking on a matter of public concern, and if that
15 outweighs the Government's interest in having an
16 efficient workplace where people aren't spilling
17 everything that is going on inside the work. With
18 respect to personal use, non-public concern matters,
19 where you are not speaking about anything job related,
20 I think you may have the right to do that. But again,
21 it's going to depend on whether you are, let's say,
22 you are speaking about your sex life, that has nothing

1 to do with your job, but it may bring disrepute on
2 your agency. And, if that is the case, then you may
3 not have a right to engage in that speech and, your
4 employer may be able to take actions against you.

5 A. MS. CRAMER: I just want to add one of my
6 other duties is doing the MSPB leg issue of whistle
7 blower cases. And, if as a Federal employee, you are
8 going to make an allegation of waste, fraud and abuse,
9 if you put it on Facebook that probably doesn't get
10 you whistle blower protection. Should you have to get
11 it to the IG, or GAO, or Congress, or someone who can
12 take action? So, that is not going to protect you
13 from getting terminated or something along those
14 lines. So, that doesn't give you the whistle blower
15 protection under the MSPB route. So, that's, you
16 know, an important thing to think of when you are
17 doing that. Also, on the immigration issue and the
18 security issue, if you've consented to a background
19 investigation, you've limited your rights anyway to be
20 investigated. You know, if you go in for your
21 clearance, they have a right to talk to your
22 neighbors, and everyone who knows you, and find out

1 everything. So, you've also consented to being
2 investigated. So, that could impact what you put on
3 Facebook or Twitter, and the investigators might be
4 able to read that, and use that in your investigation.

5 MODERATOR KENNEDY: Okay, Peter is going to
6 address Claire's second question, and we've run way
7 over so, I am going to have to limit it.

8 A. MR. SWIRE: So there is a question about
9 using, about intelligence gathering functions of
10 agencies. There is some agencies specific rules.
11 There's an FBI guidelines historically that puts
12 limits on intelligence gathering within the United
13 States. Those were changed substantially in the last
14 couple of years. There is a number of agencies, such
15 as, the CIA that under limits about domestic
16 surveillance. DOD has rules in that area also. But,
17 I don't know the DHS authorities, but it depends on
18 your agency's authority as a main limit on that. And
19 then, sometimes there is overarching First Amendment
20 limits on how much. But, if it's in the public
21 domain, chances are that Federal employees can look at
22 that, unless there are some agency restrictions on it.

1 Panel 5: What are the privacy best practices for
2 Government 2.0?

3 MODERATOR LEVIN: Well, I don't know about you
4 but my head is still buzzing from all that I learned
5 from the last panel. It was really terrific. Okay,
6 the purpose of this panel is to explore the best
7 practices for Government use of social media. In
8 light of the legal privacy and security issues that
9 we've been addressing for the last day and a half,
10 just to, I'm only build on the metaphor that for the
11 Kundra and John Kropf yesterday used about the Oregon
12 Trail and the expedition across the continent. This
13 panel hopefully will provide that roadmap that
14 will takes us all the way to Oregon. But there's
15 still some bumps in the road and some valleys
16 and mountains that we may not have figured out exactly
17 how to get over, but we're going to try and do our best
18 in this last panel. Let me just run through quickly
19 our esteemed panelists. Peter Swire, whom you heard
20 already a few times during this workshop and are
21 always happy to hear more, Ari Schwartz from the
22 Center for Democracy and Technology, David Temoshok

1 from GSA, General Service Administration, Lena Trudeau
2 from National Academy of Public Administrators. I
3 want to posit from this panel that we look at the fair
4 information, oh, Earl Crane, sorry about that.

5 (AUDIENCE LAUGHTER)

6 MODERATOR LEVIN: You know what, I didn't see,
7 Peter was sitting right there and I just couldn't see,
8 Earl. How could we forget security? We can't.
9 Privacy and security are attached at the hip. My
10 apologies. What I'd like to posit is that we look at a
11 set of principles, the Fair Information Practice
12 Principles as perhaps providing us a roadmap to help
13 us consider how we address privacy in this new
14 media. You should have a copy of the guidance
15 memorandum that the Homeland Security Privacy Office
16 issued back in December. And those principles are
17 well established. The guidance memorandum describes
18 the background for the principles and then the DHS
19 articulation. I would say that these eight principles
20 build on the Privacy Act but they in fact
21 go a little bit farther in setting out and
22 recognizing those particular considerations of our

1 electronic information and recognizing the importance
2 that privacy has in all the activities that
3 Federal agencies do when we're looking at identifiable
4 information. Each panelist is going to talk about
5 different principles and chime in as well on each
6 other's points but let me just see if we could
7 have some sort of agreement from the get go that do
8 you think these principles can provide a roadmap for
9 us going forward? And I'll start with, starting with
10 Earl, just let us know, do you think this is, in
11 particular with your area of expertise in security and
12 security has always been an important aspect of the
13 FIPPS principles. Do you see this as a possible
14 roadmap?

15 EARL CRANE: Sure. One of the interesting points
16 you have in your principles is that your group will
17 protect PII and all media. And one of the things in
18 the Security Office we do is work closely with the
19 Privacy Office and with Toby in responding to any sort
20 of privacy incidence and so we'll talk a little bit
21 more about that, issues of potential privacy
22 disclosure. So security and privacy often times work

1 hand in hand as we both seem to be the ones that pipe
2 up and say hold on, you can't go quite so fast, let's
3 think about what you're doing before you get too far
4 down the road.

5 MODERATOR LEVIN: Okay, Peter what about you? Do
6 you think FIPPS can provide a roadmap, a useful
7 roadmap?

8 MR. SWIRE: Well sure, since FIPPS was started in
9 what was then called HEW in the early 1970's now HSS.
10 They've been accepted through the OECD guidelines of
11 1980 and so one huge advantage, two huge advantages
12 for the guidelines are, one is there is a lot of
13 international consensus about them and the second is
14 that they provide a handy checklist on what
15 the issues are. The one caveat, the one thing to note
16 is that certain ones come in for closer scrutiny at
17 different periods. You know what secondary use means
18 over time, what data minimizations mean over time,
19 that'll change with different technology eras and
20 we'll get into that more as we get into details.

21 MODERATOR LEVIN: Ari?

22 MR. SCHWARTZ: Yes, I think that FIPPS are kind

1 of a necessary starting point to have a discussion
2 about the different principles put in place but as
3 with all sets of principles you need to get into how
4 they get implemented and how it works and there's
5 different ways to implement them so you could, an
6 agency could clearly be saying they're following all
7 of them and in certain ways may not be sufficient
8 and you could have other agencies that are focusing on
9 certain ones that are very relevant to a particular
10 technology and could be protecting privacy pretty
11 strongly. So I think it depends on the situation.

12 MODERATOR LEVIN: Okay and we'll get into
13 implementation in just a second. David?

14 MR. TEMOSHEK: Yeah, I guess I would say that
15 that's relevant for this discussion but in the context
16 of this overall workshop that this, we're talking
17 about the Government's use of third-party providers.
18 So within that context, I would like to discuss the
19 implementation aspects and how we as Government might
20 look at what we regard as requirements under the
21 Privacy Act and other requirements that we might
22 assert into a third-party implementation.

1 MODERATOR LEVIN: Okay, Lena?

2 MS. TRUDEAU: I agree with what the other
3 panelists have said. I would add that I think it's
4 important we see them as an ecosystem. These
5 principles work together in ways they would not if we
6 took them individually. So for instance, transparency
7 is a necessary but not sufficient condition for
8 accountability. We can't have accountability unless,
9 I believe, that unless we have some level of
10 transparency. I would add also that Peter's comment
11 is very well taken. It's something we need to look at
12 over time as technology changes. We need to make sure
13 that we're reviewing these frameworks and principles
14 that we apply to insure they're still relevant and
15 sufficient.

16 MODERATOR LEVIN: Okay, with that said, let's
17 start first with the transparency principle,
18 the principle being that Government should
19 be transparent and provide notice to individuals
20 regarding its correct use, dissemination, and
21 maintenance of personally identifiable information. So
22 Peter, how should the Government provide transparency

1 both with regards to when it's at the .gov Web site and
2 when it's working with third-party service
3 providers?

4 MR. SWIRE: Well, one topic, one point that came
5 up yesterday is there's going to be times where the
6 third-party service provider may not change its
7 policies as much as privacy advocates would want or
8 as much as fair information practices might lead to.
9 Agencies have the choice of saying at that point our
10 policy is not to ask Facebook, YouTube, whoever it is
11 for certain information; and so for people who are
12 negotiating terms of use, if you don't get some of
13 the protections you think you ought to have from the
14 terms of use, there's this important option for the
15 Government agency to bind itself publicly by saying we
16 won't do certain things. I'm not sure that's happened
17 yet but I think it's something that DHS and other
18 agencies really can consider here.

19 MODERATOR LEVIN: Any other thoughts, anyone else
20 want to add on transparency issues? David?

21 MR. TEMOSHEK: Yeah, I want to kind of reinforce
22

1 the point that Peter just made. And this has come out
2 in a number of panels in the discussion over the last
3 day and a half but we're looking at both what the
4 Federal Government does in disclosing information but
5 also looking at what information the Federal
6 Government may otherwise collect. And those are two
7 completely different things and in terms, I'm thinking
8 may necessarily provision in terms of agreement
9 specifically for what the Government would collect or
10 for what the Government would disclose because that's
11 pretty much within your own policies for how you
12 implement your services and your relationship to any
13 provider. Both of those, what you disclose and what
14 you collect and otherwise would use and retain are
15 within the authority of Federal agencies.

16 MR. SCHWARTZ: Could I just add that I think that
17 agencies can be very creative in this area, I mean
18 there's a lot of room, obviously not all of these
19 areas can be creative but in this area in particular,
20 yesterday we heard from FEMA, Jodi who was talking
21 about how they put the policies on the info section of
22 the Facebook page which I think is, I mean it is

1 basically the front of, the front section, but it was
2 in a place that was relevant to users where they would
3 want to know and be able to figure out information so
4 that's something I hadn't seen companies do on their
5 Facebook pages but Government agencies you know
6 experimenting in that way I think makes sense.

7 MODERATOR LEVIN: So what about the traditional
8 convention of notice in the bottom, in that small link
9 at the bottom of the page? Is that adequate when
10 we're doing, when the Government's engaged using
11 service provider's tools and they have a channel or
12 page on a third-party service providers, is it
13 sufficient just to have the notice at the bottom of
14 the page in the link? What are your thoughts? Lena?

15 MS. TRUDEAU: You know, I don't think it is. I
16 think that we're capable of a lot more and I say that
17 knowing full well that we have notices in links on the
18 bottom of the pages that we have used for dialogs
19 where we've engaged people in the public and we're
20 always looking for ways to do that better and be more
21 creative. But I just want to add a couple of things
22 about transparency. When we're talking about this

1 issue without really I think having a common
2 understanding of what it means. A lot of people use
3 transparency to relate to availability of information
4 in the form of data but there's processed transparency
5 as well that I think is increasingly important. It is
6 important for people when you're engaging them in
7 giving their feedback around an issue to understand
8 why they're being engaged, what that's going to be
9 used for, what the decision criteria are ultimately
10 for the outcomes of that process and I think that
11 where we fall down particularly is around processed
12 transparency. I would note also that GSA recently
13 prepared a newsletter that has a number of articles,
14 very interesting and informative articles around
15 transparencies generally is an issue. It's available
16 on the GSA Web site and I would really point people to
17 it as a good resource.

18 MR. SWIRE: So you ask if the link at the bottom
19 of the page is good enough. That's notice that you can
20 get to if the user feels like searching for it at that
21 moment and clicking on it. There's, there's another
22 familiar thing for Federal Government agencies that

1 the techies have taught me to call it interstitials
2 but it's the, you know, when you're leaving a Federal
3 Web page to go to a non-Federal Web page, the norm is
4 to have a box pop up saying you are now leaving this
5 Government site and going over here. There's a
6 question going forward of what should be in the
7 interstitial. Right, if you think there's a privacy
8 issue that's big enough maybe that should be. If you
9 think that it's important to highlight access for
10 people with disabilities, then that could be. That
11 might drive the people who have to write the
12 interstitials a little nuts as you try to load more on
13 to it but that's sort of just in time notice. Notice
14 at the time something of importance is happening is an
15 opportunity that you can consider using. I'm not
16 saying it's the right answer for privacy all the time.
17 I think that might be a burden especially when people
18 are pretty much getting what they expect. But the
19 more that it's a surprise the more that it's something
20 the user wouldn't expect, the stronger the argument
21 for that just in time notice perhaps for the
22 interstitial.

1 MODERATOR LEVIN: All right.

2 MR. CRANE: It might not be security related but
3 there is a question of when do people want to actually
4 adopt the technology. It seems like the privacy
5 concerns are relevant only when it affects you or when
6 it becomes relevant to you. The reason I bring this
7 up is there's a number of other technologies out there
8 that are specifically meant for privacy. How many of
9 you heard of P3P or privacy bird? Excellent, so a
10 fair number of people. So there's technology out
11 there that's able to support, to supplement the user's
12 decision making process to make sure that a Web site
13 you visit actually follows the privacy controls rather
14 than you having to click on the link and read the
15 privacy profile and interpret it for yourself. So the
16 question I put out there is why it has not seen
17 widespread adoption? Why is it not integrated in the
18 mainstream browsers where the first thing you do when
19 you open up your browser is set your privacy controls
20 and every time thereafter every Web site you visit you will
21 get a notice as to whether or not that Web site meets with
22 your predefined privacy controls? I'm surprised that

1 hasn't taken on the level of adoption. But we still
2 have the discussions of what we should or shouldn't do
3 and provide notice.

4 MODERATOR LEVIN: Okay, Lena.

5 MS. TRUDEAU: I would just add quickly as well
6 when we talk about the information we provide on sites
7 whether it's links or any interstitials, we're all
8 making the assumption that people can understand the
9 information that we've put in there. I think that in
10 this particular case, plain English is a really good
11 friend of ours in making sure that we're really
12 transparent.

13 MODERATOR LEVIN: Let me just mention, I saw a
14 few chuckles in response to Earl's question
15 about why these tools that allow you to
16 set your preferences haven't taken off. And I think
17 in many respects, usability issue, a lot of people
18 haven't, don't really understand how to use some of
19 these tools. Although some companies have experienced
20 a lot more success with giving customers the
21 ability to fine tune settings. Some companies have
22 more success than others but there is interest now I

1 think, so if people re-examining the usability
2 issue and trying to figure out now maybe finally where
3 may be ready to have some more tools that can make it
4 easier for people to set preferences.

5 MR. SCHWARTZ: I mean I worked on the P3P spec
6 and have done a lot of work to try to promote it but
7 I'll say that I think the failure is really in the
8 fact that Web sites didn't adopt it and then that the
9 browser makers didn't because the Web sites weren't
10 adopting it, the browser makers didn't feel the need
11 to include it into the browser so you don't have
12 mainstream consumers looking for the tools because
13 it's not coming from the browsers so there hasn't been
14 the pressure. It has less to do with users out there
15 saying having feeling comfort around the privacy issue
16 as it is around the fact that there hasn't been a good
17 implementation where we've really been able to see
18 whether users would like it or not. So I think it's
19 still up there for companies to push it forward if
20 it's going to be successful.

21 MODERATOR LEVIN: So should Government's policies
22 with regard to privacy follow the Government where it

1 goes so that when they're now moving to using social
2 service, social media services, what privacy policy
3 applies? Is it that the Government's privacy policy?
4 Is it the third-parties' private policy? Do both
5 apply? Then what's the poor consumer to do to sort
6 that out?

7 (LAUGHTER)

8 MR. TEMOSHEK: I'll start on that one because
9 this question which has been explored by a number of
10 panels, does the Privacy Act apply to non-Federal
11 third-party providers, who owns the data, what does
12 the concept of data administration mean? I'll try to
13 take a different cut at that than the discussion
14 that's occurred so far. One of the ways to look at
15 the question of does Federal privacy policy apply,
16 Privacy Act and other requirements, are the services
17 being performed inherently Governmental function
18 and is the Government contracting for the performance
19 of that function? As so whether you call it a System
20 of Records or the collection and maintenance of data
21 or the administration of data, let's just call it
22 that, or the administration of data that happens to

1 include PII. But to the extent that the Government
2 has contracted with a contractor to serve as the
3 Government's agent in performing a Governmental
4 function, that agent is clearly governed by the policies
5 of the Privacy Act. And for all sakes and purposes,
6 the agency that's contracting for that service should
7 put that requirement into the contract provisions.
8 It's when you get outside of acting as, in performance
9 of an inherently Governmental function collecting,
10 maintaining, administering data by the Federal
11 Government that you get into the question that's being
12 explored by the panels. And so the discussion has
13 been and I hope we can revisit this issue during this
14 panel, Toby. The discussion has been can things like
15 terms of service agreements which are standard
16 commercial terms of service agreements, and in this
17 case, no fee service agreements with the media
18 providers that GSA has entered into or negotiated in
19 terms of service agreements, can they include other
20 forms of Government requirements like privacy? I
21 would contend that throughout this Workshop we've
22 heard a number of different requirements that the

1 Federal Government might assert. Privacy
2 requirements, security requirements, 508 accessibility
3 requirements, green 19 requirements so I would contend
4 that the Government could do that but it requires
5 negotiating terms in service agreements that have to
6 be in the best interest of both the Government as well
7 as the third-party providers. They're operating on
8 the basis of well, making money. So if we can come
9 back to this issue and how that might be accomplished
10 and how policy requirements was that there was privacy
11 or others might be asserted in this environment.

12 MODERATOR LEVIN: Okay, Ari.

13 MR. SCHWARTZ: I strongly agree with that point
14 and I actually, I liked everything Kirsten said in
15 the last panel except for her point
16 that agencies can't negotiate with companies. I
17 think that that's just wrong. They may not be able to
18 do it for one project, one at a time, but they can talk
19 to the CIO, go to the CIO Council, have the CIO
20 Council work out issues, work out different issues,
21 working together. You can
22 work with GSA to come up with solutions in that space.

1 The White House, we've seen the White House do it.
2 The White House did it with Google. Just on YouTube,
3 there was a lot of talk about that yesterday too. So
4 we know that when agencies work together, you
5 can change the practices of the companies by working
6 out agreements. But if you're thinking about just
7 one project, of course they're not going to say that.
8 They are not going to change their entire terms of service
9 just for you for that one project.

10 MR. SWIRE: Couple of points here. So one
11 possibility is you could have negotiations to the
12 terms of service and if you have whitehouse.gov and
13 GSA working together and saying the whole Federal
14 Government is what you get if you play here, then some
15 but not all companies will go along with that and so
16 that's a decision really at a negotiating political
17 level whether to do that. There is a second
18 level you can do it if you think it's important. You
19 could have a statute that says it is required, right?
20 And by the way, if that statute happened, the
21 companies that wanted to play along would agree
22 because it would be required and the advantage of it

1 being required is that you can get them to say they
2 only get to play with the Feds if they meet this
3 privacy requirement, or this 508 requirement but we all
4 know that there's certain problems with statutes,
5 right? Possibly it might be a good rule today and a
6 bad rule tomorrow. Might be, maybe even the cookies
7 policy was decent in 2000 but it's not ten years
8 later. And so, you want to be a little careful
9 certainly with anything that's not technology neutral.
10 You want to be careful going forward with the statute.
11 But on any specific piece, one of my big themes for
12 these two days is, if there's any specific piece where
13 statutes would help, I think there would be an
14 openness at senior levels to at least hearing that
15 case and if it's a convincing case for a statute, I
16 think there would openness in Congress for letting the
17 Government update its practices for this new age. So,
18 if you see a statute that would help, let the world
19 know about it, and then maybe we'll see the changes in
20 law instead of being stuck with lousy old laws.

21 MODERATOR LEVIN: Okay, so I gather part of that
22 actually responds to the concern that you may have

1 such a range of practices, Government policies,
2 privacy policies at one level, corporate policies might
3 be a different level but through some way to get them
4 some consistency here so that the public, the American
5 public doesn't have multiplicity of policies that
6 they're trying to figure out what applies. Okay,
7 let's look now at the second principle which is
8 individual participation. The Government should
9 involve the individual in the process of using PII, to
10 extent practical, seek individual consent for
11 correction, use, dissemination, and maintenance. The
12 Government should also provide mechanisms for
13 appropriate access, correction, and redress regarding
14 use of PII and that's a slight variation. I'm
15 reframing them a little bit for purposes of this
16 discussion as opposed to the DHS iteration that you
17 have. Okay, so with that in mind, how can the
18 Government provide for individual participation? Ari?

19 MR. SCHWARTZ: Well, usually this discussion
20 comes down to opt-in versus opt-out and, which is in
21 my mind some what unfortunate because we won't have
22 time today to get into details about all the different

1 kinds of opt-ins and opt-outs that there are. There
2 are such thing as an opt-in that's bad for privacy
3 and there's such a thing as an opt-out that's good
4 for privacy and this is all on some kind of spectrum
5 where there is good and bad. But generally it gets
6 boiled down to opt-in is good for privacy and opt-out
7 is bad for privacy, so with the time that we have,
8 I'll leave it focused in that way. I want to
9 first of all comment on the fact that Earl
10 made a good point yesterday on the security panel
11 about the move from a systems-based approach to
12 solving some of these issues to a use-based approach.
13 I think that makes sense for security and it makes
14 sense for privacy, make sense for information policy
15 in general and especially in this area. If we can
16 come up with uses where we can get the right kind
17 of individual participation for that particular use,
18 that makes sense for that use and then have the other
19 fair information practices kick into place as we need
20 them to account for the failings of individual
21 participation in certain areas. That would be helpful.
22 I'll give you an example, the example of there has

1 been a lot of discussion on analytics, and it's very
2 difficult to get opt-in to do broad scale analytics on
3 Web sites, for individuals that are coming in
4 trying to figure out where individuals go. There's
5 different kinds of analytics obviously out there, and
6 they're used for different purposes and some are
7 probably easier to get opt-in for, some are going to
8 be more difficult to do that for. So what should the
9 rules be? CDT and EFF worked on a paper to try to
10 come up with some of those rules, and we said that it should
11 be opt-out. We also came up with another set, double
12 set of fair information practices that need to go into
13 place if you're going to make it opt-out. In this
14 context, and that's to make sure that that information
15 that is being collected isn't being used for multiple
16 purposes beyond what users would expect it to be in
17 other rules. So that's one example. Now, I haven't
18 heard too many other good examples where people
19 think that persistent identifiers should be used in
20 an opt-out capacity, right? If you can come up with
21 another use where it's difficult to get consent
22 regularly, then you should do that.

1 You should let people know that because, what
2 we've been hearing, at least from people who have been
3 paying attention to this, is we see a lot of case
4 examples where opt-in is actually regularly in use
5 even in the commercial sector. Comments for a blog
6 for example, most of them have a little "remember me"
7 check box that's unchecked that people have to
8 actively check it. That is an opt-in, right? So we
9 are seeing this. The examples that we have been
10 hearing from agencies about what they want to do with
11 persistent cookies with logins, etc. and things where an opt-
12 in seems to make sense except with the exemption of
13 analytics.

14 MODERATOR LEVIN: Are there any other examples of
15 tools or implementations of choice that you think are
16 worth bringing to people's attention? What are ways,
17 you've mentioned the check box with comments, are
18 there other examples where you're able to give
19 individuals the opportunity to exercise choice as
20 easily as that?

21 MR. SCHWARTZ: There are a lot of examples out
22 there where the opt-in is very easy. I think there's

1 also this question of how much this ties to data
2 minimization -- in some ways about how much you need to
3 collect to do the actual function of what you're
4 trying to do. But we see examples where
5 you give people a choice at the bottom where
6 they can say what they wanted, as they're filling out
7 a form, they have a few different options. One of
8 them is yes, I want to be remembered, I want you to
9 remember me, and another one is just submit this data
10 and I'll refill out the form again next time. The
11 individual is making the choice at the time that they
12 submit the data on a form. Shopping carts is another one.
13 Distance learning is another example where you may
14 want to store information over different sessions
15 for certain purposes and give people a choice about
16 whether they want to do that at the time that they
17 submit information or when they've finished the
18 chapter of the course or something like that. People
19 are used to that. That's what happens in the private
20 sector as well.

21 MR. CRANE: Ari, you asked for examples where
22

1 opt-out is difficult to do so in your persistent cookie
2 yard, you're going to find out that right.

3 MR. SCHWARTZ: Not where opt-in is difficult,
4 where an opt-in would be difficult and wouldn't work.
5 That's what I'm saying.

6 MR. CRANE: Okay. I think I misunderstood.

7 MR. SCHWARTZ: I'm saying that the only case that
8 I've heard where opt-in doesn't work in the Government
9 from what Government agencies seem to want to do is
10 analytics. But where they need to collect information
11 from everybody and where people opting out would, if
12 there were large numbers about those, it would make
13 providing this particular service difficult.

14 Okay, so actually I just said it wrong but an
15 example, a couple other examples that come to mind is
16 telephone records for example. I don't know if I'm
17 off base with this or not but every time you place a
18 phone call, that phone call is recorded and that's a
19 mechanism for billing. So being able to do that
20 anonymously is something that would not be possible
21 without having any sort of sense of the billing
22 environment. And another one that comes up from a

1 gentleman I had this conversation with in the audience
2 is logging when you visit a Web site. For the same
3 reason as analytics, so you know who visits the
4 Website, it's a standard security practice and has
5 been for years to log the visitors to your Web site so
6 that if anything happens to that Web site you have a
7 mechanism to go back and perform forensics and try to
8 figure out what happened that broke the Web site
9 particularly if it's a malicious attack. There are
10 certain exceptions where there's no participation
11 at all allowed and security is obviously one of them.
12 So the question is how much information do you need
13 to perform that task and not so much whether an
14 individual has the ability to stop that information
15 from doing it. So we focus on this again, focus on the
16 use. I'm not counting and talking about the opt-in
17 and the opt-out, I'm not talking about the places
18 where there are current exceptions in pretty much
19 every policy.

20 MODERATOR LEVIN: I want to come to the IP
21 address when we talk about data
22 minimization. Let's look then at the purpose

1 specification in the third principle. Where the
2 Government should specifically articulate the
3 authority that permits the collection of PII and
4 specifically articulate the purpose or purposes for
5 which the information is intended to be used. How
6 important is that principle in this context with
7 social media and when does the Government need really
8 to collect PII in order to provide a social media?
9 Lena, can you start us off?

10 MS. TRUDEAU: Well, you know, I'm going to sound
11 a bit like a broken record here because I'm going to
12 go back to the point Ari was making which is, I think,
13 that it has a lot to do with what you're undertaking
14 and the kind of information you're collecting.
15 There's some information that is more sensitive than
16 others, there's some information that's required less
17 often. So, for instance, in some of the dialogs that
18 we've been running at the National Academy, we require
19 a valid e-mail address in order for people to register
20 for an account. Now we allow them to choose whatever
21 screen name they would like, and we do not share that
22 information with anyone else outside the National

1 Academy, and we aggregate things before we report on
2 data back to our clients. So there are a number of
3 protections that are built in there, but there are
4 times when you want to be able to understand that an
5 individual is at least an individual if you're trying
6 to get some sort of input, at the front end, of
7 what is potentially a policy development process.
8 But I think that those are the situations where
9 making the use of the information clear to people,
10 helping people understand what you are collecting
11 and why, and how it will be retained and protected
12 is really, is really important.

13 MODERATOR LEVIN: What about, and this was
14 related to a question that came up in the last panel,
15 in terms of articulating the purpose. What about
16 unarticulated purposes? Use of this information
17 that's publicly available for purposes beyond the
18 specific mission for which the information was
19 provided, whether it's used by law enforcement, used by
20 intelligence agencies, used for fraud prevention, or
21 other uses. Should it just be a given that
22 the public should recognize that whenever they're

1 posting information that it may, in addition to
2 the purpose for which it's specified in the notice,
3 that information may also be used for a host of
4 other Governmental purposes? How do we address that?
5 Is that just an educational concern?

6 MR. SCHWARTZ: I would say there are some
7 exceptions in the Privacy Act. I'm not saying this is
8 all going to be covered by the Privacy Act but there
9 are some exceptions clearly in the Privacy Act for
10 different uses of information. I would think that
11 we can come up with a series, of user expectations,
12 what users should expect that the information
13 is going to be used in a certain way, and there're
14 written down somewhere. Right, it's not just
15 someone thinks that users expect it. We think users
16 expect it and we're going to write those expectations
17 down somewhere and make it clear to people that's
18 where, that there are exceptions for these uses.

19 MR. SWIRE: So, just to use a term that lots of
20 people in this room heard a lot about the last few
21 years and haven't heard very much at all for the last
22 two days, information sharing. Right? Pretty big

1 theme over the last seven or eight years in the
2 Federal Government and a presumption of sharing said
3 the Markle report as a way to overcome barriers between
4 agencies. So there's a question about how, whatever
5 we're discussing here, whatever counts as 2.0, where
6 we're in a privacy related conference and tend to be
7 pretty careful about user data, how that's going to
8 fit in with this information sharing environment and
9 all of the very long meetings and presidential
10 directives and stuff like that we had over there. And
11 I doubt in this panel or this two minutes on purpose
12 we're going to solve that, but I just want to flag that
13 that while the 2.0 people and the privacy people are
14 moving forward on certain things, there's a lot of
15 people in the Government who've had information
16 sharing as their, as very high priority and they
17 didn't suddenly stop on January 20th for lots of good
18 reasons. Right, there's a lot of reasons to share
19 data and so in that information sharing world, purpose
20 specification hasn't been the holy grail all the time.
21 There's a lot of skepticism about that. So I just
22 point out there's some other areas of discussion in

1 the Federal Government that we haven't focused on this
2 much here.

3 MODERATOR LEVIN: So who said privacy was easy?
4 It's not, it's very challenging. Okay, fourth
5 principle on data minimization. The Government should
6 only collect PII directly relevant and necessary to
7 accomplish a specified purpose or purposes and only
8 retain PII's as long as necessary to fulfill the
9 specified purposes. All right, so how does this
10 principle conflict with the very nature of social media,
11 which is to encourage a lot of interactivity, a lot of
12 communication and really not data minimization? And
13 what limitations if any should the Government place on
14 its own collection of PII or with regard to social
15 media?

16 MR. SCHWARTZ: I asked Toby to be able to speak
17 on this. I gave a talk recently where I said that
18 data minimization is one of the key privacy
19 principles, it's one of the fair information practices and
20 that roughly speaking Web 2.0, you can think of it as
21 data empowerment. That data is going to set users
22 free and let users with all their cool tools do all

1 these things they've never done before, user generated
2 content and communities that come out of that. And so
3 I suggested in that talk that there's an important
4 conflict between the tradition of data minimization
5 from privacy and the view of data empowerment for 2.0.
6 And I've been going around to privacy experts and 2.0
7 experts since then saying please, please research
8 this, figure it out because I don't know how to
9 resolve that conflict very well. I've just a couple
10 of additional points. One point is, one reason the
11 privacy people have often given for data minimization,
12 I've heard this over and over again in privacy
13 conferences over the years, is that storage is
14 expensive. It's hard to find data, if you take too
15 much of it, so you should be very careful and only ask for
16 what you want for. However true that was ten years
17 ago, it's a lot less true today. Storage has gotten
18 cheap and search capability has gotten much much better,
19 and destroying data is actually expensive. It's hard
20 to figure out how to actually destroy it. So I think
21 that convenient privacy conference trope, oh it's
22 better not to keep it because it's too expensive to

1 keep, I don't think that's factually true very often
2 anymore. And I'm seeing some nods from some people
3 in the audience as I was saying that. So, that's too
4 bad because it would be convenient to say it's
5 efficient to data minimize because then you get
6 privacy. I don't think it's efficient to data
7 minimize, and so I think that's a problem in this area.
8 There are some times when it's efficient to data
9 minimize. If you're under data breach laws and you
10 got a whole bunch of credit card numbers and you're
11 not able to keep it secure, then you're going to get
12 hammered with data breach notifications when you screw
13 up. And so certain data breach triggers medical
14 information increasingly and credit card numbers and
15 SSNs, there are reasons to minimize those because it's
16 hard if you have a data breach. And I have another
17 article called Peeping Right Now which talks about
18 insider breaches, and if you're worried about your
19 employees looking at the passport photos of Obama or
20 looking at the medical records of George Clooney, then
21 those are reasons to mask and minimize because you're
22 going to get in trouble when your employees look at

1 stuff they're not suppose to look at. So there's
2 reasons to minimize in certain subsets, but I think
3 it's a big challenge to the privacy fair information
4 principles to say data minimization should be the norm
5 when an awful lot of the Web 2.0 people are
6 celebrating the uses of data. I think in the
7 Government context though, it still is somewhat
8 expensive to keep data, not expensive in the
9 cost realm, but it's expensive in the list of things
10 you need to do with the data. You can look at
11 Alex's slide from the last panel where he tried to list the
12 laws that filled that half of the screen and which
13 of those laws kick in and at what time. And if there's
14 one thing that Privacy Impact Assessments have really
15 been - - give Peter credit for being the first one
16 to highlight them inside the Federal Government is, saying
17 when you collect this type of information, have you
18 thought about the consequences of collecting this
19 type of information? You can collect it, but what is
20 the impact to the citizen and what is the impact
21
22

1 to this law or regulation in this context? And so
2 it has been successful not in as you can't do
3 this, but in here are the other things you're
4 going to have to deal with. I've been hearing
5 from Web masters who say look, we know that
6 when we do certain kinds of authentication, all of
7 these different laws and procedures are going
8 to kick in. So we would rather authenticate
9 less and keep less information about individuals
10 when we can. Right? And we only authenticate up
11 to the level using the GSA levels as the guide
12 that we need to authenticate to because otherwise
13 we're going to have to have all these other things
14 kick in. So, you think that we have had one
15 place where we have been successful here already
16 in data minimization is the ability to point out
17 where the different laws come into play and the
18 Government act needs help with that.

19 MR. TEMOSHEK: And on this point on data
20 minimization, but I think broader across the different
21 fair information principles, one of the aspects that

1 this panel brought up as well as the security panel
2 yesterday was the issue of Privacy Impact Assessments.
3 I think Privacy Impact Assessments are part of a larger
4 requirement for how we assess and determine security
5 vulnerabilities and information systems as well as the
6 data that's being recorded. To the extent the data
7 collected from any source is maintained by the
8 Federal Government and information systems, they're subject
9 to security assessments as well as Privacy Impact
10 Assessments under the Federal law -- Federal Information
11 Security Management Act or FISMA. But the point where
12 that interchange of data is outside of a Federal
13 boundary becomes very critical in how we assess the
14 information system but also how we assess privacy impacts.
15 In establishing the boundary of where information is collected,
16 where it's transferred, where the Federal Government enters into
17 that environment and where it's outside the Federal
18 Government's control and what does the Federal
19 Government expect for any of those providers in so far as
20 Privacy Impact Assessments and or security assessments
21 for what sits outside the Federal boundary.
22

1 MODERATOR LEVIN: Before we leave data
2 minimization, I want to talk a little bit about
3 retention policy so when we're negotiating terms of
4 service agreements, an issue that's come up is
5 retention policies with regard to the information
6 that's collected if it's a third-party service
7 provider. We've seen over time that it used to be that we
8 would keep data till the cows come home. Gradually
9 commercial companies have been reducing
10 retention policies to nineteen months and now
11 we're seeing some as nine months. Several key
12 companies have reduced retention of PII and Web logs
13 to as short as nine months. What's the Government's
14 role here with regards to retention policies, not only
15 for itself, but also for the third-party service
16 providers?

17 MR. SWIRE: My guess is that your security folks
18 are going to want to keep their logs for at least a
19 little while. Is that right?

20 (LAUGHTER)

21 MODERATOR LEVIN: What do they need to keep in
22 the logs?

1 MR. CRANE: The answer to the question is what is
2 it that's going to be retained in that log.
3 A lot of the time you use the seven year
4 rule, but in a lot of cases we don't have
5 the capacity to store that much. One of the things
6 that you look at is full packet capture. If you're
7 capturing every piece of information going in and out
8 of your organization, which Federal agencies should do
9 and if they haven't started doing it yet they will
10 underneath the TIC, is looking at what information will be
11 retained and what wouldn't be retained. And the whole
12 issue of minimization once you're capturing that much
13 information becomes a huge deal. And figuring out
14 what can be retained so that you can figure out what
15 happened and what shouldn't be retained and
16 then how long that should be. So it's just not an
17 issue of space but it's also goes back to your issue
18 of minimization.

19 MODERATOR LEVIN: Well if we have to keep
20 lots of information for long periods of time in order
21 to be able to go back to deal with specific incidents
22 and I'm not sure that that's actually always the case.

1 That brings us to the next big principle which is use
2 limitation. The Government should only
3 use PII for the purpose specified. So what kinds of
4 use limitations do we put on all that data that we're
5 collecting, if any?

6 MS. TRUDEAU: I'm going to jump in on this one
7 and actually I want to tie this back to data
8 minimization for a minute and I guess what I want to
9 say is so I'm not a lawyer and so please forgive me if
10 I get any of the real specifics wrong here and I'm
11 happy to have anyone point that out for me, but there's
12 another issue that we're dealing with here which is on
13 some level there are situations now where we collect a
14 lot of information and we have value in that
15 information that we did not realize we'd have when we
16 first collected it. And sometimes that's a really big
17 problem and sometimes it's really not. So for
18 instance, my medical records, if I'm showing
19 information about my medical records I want to know
20 that the amount of information collected is the least
21 amount required to do what needs to be done. I want
22

1 to make sure that it's used only for the specific
2 purpose for which I shared it, and I really want to make
3 sure there are a lot of safeguards around that. At
4 the same time there are a lot of forums available to
5 us online these days where people are sharing
6 information in a public forum. If people choose to put their own
7 name against something and include information that
8 when aggregated with other data might provide some
9 level of situational awareness, I am not convinced
10 that the Government shouldn't be able to use that
11 because sure as heck there are other entities out
12 there using that. What I think though, on
13 that side of the coin, that is important and something that
14 we haven't really talked about yet, which is education.
15 I think that particularly with younger generations
16 coming on line these days, people don't necessarily
17 have the same understanding of the risks to their own
18 personal privacy and security that come from some of
19 the information they're sharing, and I think that we
20 can accomplish a lot with educational efforts. So
21 that should be a priority also. I just really want to
22

1 make sure that we're making a clear distinction
2 between the kinds of information that's being
3 collected because for some, I just don't think it's
4 an issue. You know when Wal-Mart can look at the
5 Twitter sphere and understand how better to stock
6 their shelves, I'm just not sure it's a
7 problem for Government to have some more kinds of
8 functionalities in similar situations - - Where this gets
9 really tricky is when you look at applications like
10 Virtual Alabama where all of the information, I
11 mean there's some restriction on who can access that
12 system, but the information that used to be housed in
13 silos were taken together and put into an online mash
14 up, all of a sudden it provides some very interesting
15 situational awareness and uses for which I'm sure some
16 of that data was never intended. You get into some
17 tricky areas.

18 MODERATOR LEVIN: But I guess, are we talking
19 about aggregated information or identifiable
20 information, because I don't think frankly privacy
21 issues arise if it's just aggregated data. If
22 you're stripping out the identifiers then you're good,

1 if you're stripping out the identifiers.

2 MR. SWIRE: Can I speak? So, that sounds as
3 though it's a distinction that we understand but it's
4 a really, really hard one. We have data.gov as an
5 initiative of the White House right now. A lot of
6 initiatives to try to get transparency out there, get
7 views into data sets. On the other side, and this
8 gets to use limits, a lot of that is non-identifiable.
9 But on the other side there's this whole literature
10 and set of experts in the computer science world,
11 Latanya Sweeney is the best known of them, whose coming
12 up with all sorts of really good ways to take
13 publically available data and start to correlate it
14 and find ways to identify some, maybe two or three out
15 of a hundred, maybe ninety eight out of a hundred, to
16 correlate some of the people in the supposedly
17 de-identified data set and link them up to identify them in a
18 pretty strong way. This has always been a problem for
19 the Census Bureau; they have a long history of small
20 cell size and how to do it. The statistical agencies
21 are facing it, but with the proliferation a publicly
22 available data and the improvement of searches, it's

1 becoming a much harder thing to say that some things
2 are de-identified.

3 MR. SCHWARTZ: I think the answers to
4 this issue are going to change over time. There's no
5 real correct answer in this space except to say that
6 if you're taking personal data from a public space or
7 from a social media site and then you're integrating
8 it with another record, an existing record, then it is
9 under the Privacy Act, it is a Privacy Act change.
10 You have to disclose that. You have to follow the
11 Privacy Act in doing that. If you are taking the
12 information and you're tying it to another collection
13 of information you are changing the collection, you
14 need to redo the PIA, right, and make it publicly
15 available. There are some things that are in place
16 that if you are taking this information in and making
17 decisions based on it, and using it differently,
18 and using the records differently than you have before,
19 then you have to make changes in your practice.

20 MODERATOR LEVIN: But what's the Government's role
21 though when it's dealing with third-party service
22 providers that, we won't name any specific ones, that

1 have large numbers of applications of products and
2 services that an individual might use and that those
3 third-party search providers might have the ability
4 therefore to track individuals across all these many
5 different services and products so that maybe in one
6 instance with one product, they're not identifiable, but
7 because they collect the IP addresses they're able
8 to track them through their activities across other
9 Web sites. Should the Government in negotiating these
10 terms of service play any role in saying these third-
11 party search providers should not track individuals
12 across Government Web sites?

13 MR. SCHWARTZ: Well, this is probably what I was
14 saying earlier. I do think that agencies do have
15 leverage here and that they should be looking out for
16 what is best for the users of the Web sites,
17 of that particular site and they do have the ability
18 to work together to come up with and solve these
19 terms. So I do think it's up to GSA, to the CIO
20 Council to, and especially the folks in the White
21 House that are pushing the Web 2.0 initiatives, to help
22 make that happen. Large agencies I also think can do

1 that as well. I don't know, someone like the Defense Department
2 or something like that can help to promote this, and I
3 think it's hard for a particular project, one
4 particular project within an agency to say oh, we're
5 going to negotiate with Facebook or YouTube on
6 changing their terms of service. That's just not
7 going to happen, but when you talk about bigger
8 entities working together, I think that you can have a very
9 large impact.

10 MR. TEMOSHEK: Let me describe the
11 way to look at what GSA has done so far in negotiating
12 terms of service agreements. The question we were
13 looking at answering was can the Federal Government
14 legitimately enter into agreements with any of the
15 media providers that are out there today? And in
16 general, the answer to that question is no. There
17 were clauses or other terms and conditions that were
18 part of those terms and conditions that prevented the
19 Federal Government from entering into the agreement. We
20 cannot agree to indemnify individuals or companies
21 given our limitation, our fiscal limitations, to
22 establish unbounded obligations under the Anti-

1 Deficiency Act. We can't agree to define liability
2 determinations. Those are provisions that we have
3 to be able to standardize and that's what GSA did.
4 Consider it the first step in negotiating terms
5 of agreement. We didn't look at a wide
6 range of other requirements. We looked at, can
7 the Federal Government or Federal agencies or GSA for
8 that matter enter into agreements with these companies
9 on an open ended basis. That's the nature of those
10 negotiated agreements. If you want to get to
11 additional requirements, whether it's GSA that
12 continues that negotiation or other companies, the
13 Federal Government will need to be able to show a
14 legitimate process for establishing Government-wide
15 requirements. Not that this is one agency's desire or
16 requirement or another agency's requirement. The
17 companies will not alter their terms and agreements
18 based on that but on a Government-wide basis, they
19 may. Now this question, which is fundamental to the
20 business model of the companies GSA has
21 been working with, for how they manage advertising,
22

1 how they manage their services, gets into
2 the fundamental business model. And the question came
3 up yesterday. Will the Government entertain
4 establishing these types of services under a
5 Government model? And I think the answer to that
6 question from the panel was, well the Government
7 shouldn't really try to do that now. The Government
8 should try to see how they can use the infrastructure
9 that's being developed and put into place and if necessary
10 modify existing terms and agreements on behalf of the
11 Government on a Government-wide basis, which will
12 influence that negotiation process before attempting
13 to take a different path and try to build that up for the
14 Government's own purposes. So we're at that first
15 step. Yes, we can enter into these agreements; yes,
16 we can look at additional requirements, but we have to
17 consider what that does to impact the providers and as
18 well as other legitimate Government-wide requirements
19 in different arenas. And I think that's the next step
20 we look at.

21 MODERATOR LEVIN: Okay. The sixth principle is
22 data quality and integrity principle, that the Government should

1 to the extent practicable insure that PII is accurate,
2 relevant, timely, and complete. So Lena, is this
3 principle even relevant to the Government's use of
4 social media, and what obligation if any does the
5 Government have to ensure that this principle is
6 adhered to?

7 MS. TRUDEAU: I'm sure the people in the panel
8 could speak a little bit better than I could to data
9 quality and integrity but I do think it is important.
10 We're in this world where we seem
11 to think that proliferation of data is the goal. But
12 I think that what we really want is access to the
13 right data at the right time, and I think that
14 principle should to the extent possible be followed,
15 particularly when we're collecting personally
16 identifiable information. I think we should have that
17 as a basic principle.

18 MODERATOR LEVIN: Anyone else on data integrity and
19 quality?

20 MR. SCHWARTZ: I'll just say that you
21 hear Twitter is now talking about not making money
22 through advertising. They're talking about making

1 money through validating speakers. So I think there's
2 something to be said about the role of data quality
3 and social media and that will obviously point to
4 Government as well.

5 MODERATOR LEVIN: Now, the seventh principle,
6 security, Earl this is your football to catch. The
7 Government should protect PII through appropriate
8 security safeguards against risks such as loss or
9 unauthorized access or use, destruction, modification, and
10 unintended or inappropriate disclosure. How do we
11 implement that principle both in the .gov world and then
12 with our third-party service providers?

13 MR. CRANE: It's something I actually know a
14 little bit about. I'm not a privacy expert as you can
15 tell so I rely on Toby for a lot of the systems there.
16 There's really one thing I want people to take away
17 when we're talking about security and Web 2.0 and
18 that's the fact that different use cases require
19 different approaches to security. So Mark Drapeau on
20 the security panel yesterday, and we mentioned the paper
21 that he wrote with Linton Wells at NDU. One of the
22 reasons why I'm a fan of that paper is it articulates

1 four specific different use cases for social media.
2 And when we start talking about security they all get
3 lumped together and they all get confused. So the four
4 different ways are (1) inward sharing, (2) inbound sharing,
5 (3) outward sharing, and (4) outbound sharing. It can be
6 confusing to tell which one is which, but you can roughly
7 break it out into (1) using internal collaborative resources,
8 internal to the organization like Intellipedia. (2) Next is
9 having internal users visiting external sites like a dot com
10 Web site or a Government Web site. (3) Next is when the
11 Government makes data feeds available out to the rest of the
12 world, such as data.gov and recovery.gov, so that those data
13 feeds can be picked up, and the outside world has a level
14 of visibility. Though, that gets into the data aggregation
15 issue. (4) Finally we have the outside world providing
16 information using different information feeds of what
17 is happening and those are captured by internal
18 data sources. Every single one of those use cases has a
19 completely different security profile and when we lump
20 them in all together it gets confusing very quickly.
21 So your internal security should address the case
22 where you have an Intellipedia-like site

1 internally that you're using, and that would be the
2 same as if you have an internal hosted blog. I'm not
3 talking about going to Blogger.com but you have a .gov
4 Web site where you enable blog functionality. That's a
5 Government information system. It falls under FISMA
6 and there is a decent set of guidelines that provide the
7 good security controls as to how we can allow that to
8 happen and from a secure mechanism. Now, privacy, I
9 think, has a lot more issues with that situation than
10 security does because that one's rather cut and dry as
11 long as you have a decent security program. Not to
12 belabor the process, but you can roughly break that
13 into having a strong Government process, having a
14 strong compliance process through your certification
15 and accreditation program, having a good security
16 operations capability so that you actually have
17 monitoring of that information system, and you have
18 people that are able to respond if anything happens to
19 that information system if it's attacked. Now where
20 it gets tricky is one of the other completely
21 different use cases of an internal user going to Facebook
22 The privacy concern

1 I think has been pretty well articulated, but the
2 security concern is all the issues that crop up once
3 you have an internal user accessing this Web site
4 externally where you don't have any assurance to its
5 security. You don't have any assurance to the
6 controls. You don't have any assurance who the
7 members and users are on that Web site and that's where
8 it really starts to get tricky. A lot of the common
9 attack factors that start to come out are really
10 nuances, and I like Kirsten's comment from the previous
11 panel that this is stuff that we've seen before, it's just
12 a new way of looking at it. So your social
13 engineering attacks have been around since before you
14 know the Internet existed. It was, you know,
15 shamsters and scallywags, and now we have 419 Nigerian
16 scam sending letters with the Post Office and then we
17 eventually got to e-mail and now we're at social
18 engineering through Facebook. It's the same thing.
19 It's just a new media. So we need to make sure that
20 our users are educated to deal with these issues and
21 building that education program is one of the core
22 tenants of information security program that

1 is mandated under the FISMA law that you must
2 provide annual security awareness training. The
3 question is, are we providing the right type of
4 security awareness training? It tends to amount to
5 change your passwords. Make sure your computer is
6 updated. Don't post anything bad out on the Internet.
7 Well what about educating users about
8 someone that tries to illicit information from them.
9 What about them accessing social media, because we're seeing such
10 a blending of personal use and professional use.
11 They're going onto Facebook at home. Well that's an
12 attack factor because they're a recognized Federal
13 employee so now I'm going to attack their home user,
14 their home account, their home computer and try to use
15 that to get access to a Federal information system.
16 Well that's a vector you never really thought of. One
17 of the things I talk about is this concept
18 of an attack surface and in the information
19 security industry where your attack surfaces have been
20 pretty well known for years. It's how big
21 of an Internet footprint do you make, so the bigger
22 footprint you have the easier it is to attack, to hit

1 you. Just like shooting a bullet at a target. Well
2 the same thing applies for an individual as they
3 expand their Internet footprint through social media
4 and as they recognize and identify themselves as a member
5 of a Federal agency, contractor, or a Federal employee,
6 they're establishing a Federal footprint in social
7 media. That makes a bigger attack surface. The
8 bigger the attack surface you have, the easier it is to
9 attack you and the easier it is to find a way to
10 exploit any number of vectors to be able to get what
11 I'm after and usually it's information. So there's a
12 very different types of discussions that need to
13 happen when we start talking security and Web 2.0 and
14 social media. That's all I want you to take away is
15 to look at the different articulation of those use
16 cases. Thanks.

17 MODERATOR LEVIN: Thanks Earl. All right, the
18 last principle is one of the most important actually.
19 It's accountability and auditing. That the Government
20 should be accountable for complying with these
21 principles, providing training to employees and
22 contractors who use PII and auditing actual use of

1 PII to demonstrate compliance with the principles that
2 are applicable - - protection requirements. Well how
3 does the Government provide for auditing in the
4 context of social media, particularly when the
5 services, the Government services are being provided
6 by third-parties, how do we audit these practices?
7 Any thoughts?

8 MS. TRUDEAU: As an organization that provides
9 services as a third-party for Government, maybe I'll
10 start off. I do think that it's important from the
11 Government side to have strong program management and
12 oversight. I think that's really important. On a
13 broader level, I would say accountability is very
14 difficult to achieve without transparency and so I
15 think it's important to understand that it's very hard
16 to hold people accountable if you haven't done the
17 work up front to really understand what is it that
18 you're trying to accomplish, what information are you
19 collecting in servicing of accomplishing that and what
20 else is in place. What are the goals that everybody's
21 aligned around because if that's not set out up front,
22 particularly when you're working with third-parties

1 then you have a very, very difficult time on the back
2 end holding anybody accountable. Very clear
3 performance measures are also a part of that infrastructure.
4 So I would say that's the basic fabric of
5 it. At the same time I think that going back to again
6 Peter's original point about needing to revisit these
7 things over time. This isn't something that static or
8 exists only in just a moment in time and then never
9 changes. Technologies change, circumstances change
10 and that changes the privacy landscape that we're
11 dealing with.

12 MODERATOR LEVIN: What kind of due diligence
13 should Government agencies do, or GSA, as its
14 representative of a third-party service provider with
15 regard to their practices?

16 MR. SWIRE: This is one of the down sides of not
17 using procurement. Right, if you have a procurement
18 and you have standard terms, you have a variety of
19 ways to do audit and accountability. The very light
20 weight terms of use for a lot of 2.0 applications
21 aren't really designed for that same kind of
22 accountability. As any of these things become more

1 mission critical as they get rolled into service
2 provider contracts that are more important to
3 the agencies, some of this will get rolled
4 into procurement and then you'll have a chance
5 to do audit and accountability. You don't want to do
6 that too soon and stop the experimentation, but as it
7 gets more and more important to what you're trying to
8 achieve and your agency, you'll probably bring it in
9 to the procurement process eventually and make sure
10 you have these controls in place.

11 MR. TEMOSHEK: Yeah, the Federal Government over
12 the last twelve, ten years has kind of embraced the
13 concept of pursuing, I'll use the term, centers of
14 excellence. But, because it's an often used term,
15 we've called it lots of different things. This is
16 Gov 2.0, but you can call it e-gov, or you could call it
17 Government lines of business where Government does
18 similar things across the Federal Government, and in
19 order to build infrastructure and I consider
20 policies, terms of agreement, standard operating
21 procedures, that's part of the infrastructure
22 necessary in this environment. And so one of the

1 things that we've pursued over the last decade has
2 been getting to the point where each agency doesn't
3 have to build that infrastructure on its own but we
4 look to designate it, lead agencies or agencies to
5 take a lead for the Federal Government in building
6 infrastructure. Now that infrastructure may be
7 through Federal Government providers, maybe with
8 commercial providers, maybe through procurement
9 processes as Peter just described, or other processes
10 for how are the capabilities asserted to ensure that
11 Government-wide requirements that need to be met or
12 some list of qualified providers can in fact provide
13 this service so that we can direct Federal agencies to
14 that infrastructure. This type of discussion
15 kind of leads to that direction as well, but
16 the development of requirements, how those
17 requirements are asserted, as well as the assessment
18 and qualifications of capabilities against those
19 requirements becomes instrumental in pursuing how does
20 the Government builds infrastructure across the Government
21 so that the Government can use qualified services that
22 the Federal Government thinks are right as we go

1 forward and recognizing that those requirements also
2 are going to be subject to change.

3 MR. TRUDEAU: I'm going to jump on that and say
4 something that maybe David didn't want to come as far
5 out as saying, but I think there's a real role to play
6 for GSA here particularly in the development of a
7 centralized platform of applications and service
8 agreements and tools and approaches and methodologies
9 that people across Government can use. You know, it
10 doesn't always apply when you're talking about the
11 real emerging stuff but even then, GSA can play a role
12 as an incubator. If it's in the Intel space, ODNI is
13 doing a great job with the stack they've built over
14 there. You know, why does every Intel agency has to
15 recreate the wheel? In DOD, you know there's a huge
16 economies of scale to be gained, and we're
17 moving towards Government as a platform. There
18 are a lot of benefits to come from that standardized
19 terms and conditions and policies as part of that. I
20 would really, really encourage everybody in this room
21 before they go out and tackle a problem on their own
22 one more time to put your head up and look

1 around and see who else might have done this before.

2 MODERATOR LEVIN: Alright, Government as a
3 platform, well what a great thought to end with and
4 the challenge that we all have there is huge. Any, we
5 have time for just a few questions. I want to be sure
6 if there are any remaining questions that you are left
7 with that we give you a chance before I close the
8 meeting today. Any questions? Well, actually I'm
9 hoping you're leaving with lots of questions.

10 MS. TRUDEAU: Can I add one thing Toby?

11 MODERATOR LEVIN: Yes.

12 MS. TRUDEAU: I just wanted to say this is my own
13 personal view but I felt the need to say it. It's
14 actually and I'm not saying Government shouldn't be
15 concerned about this. It's absolutely the right stuff
16 about Government to be concerned about, but in my own
17 personal life, it's not the Government collection of my
18 information that I'm concerned about at all, it's my
19 credit card company and my health insurance company
20 and Google for that matter.

21 (LAUGHTER)

22 MODERATOR LEVIN: I think I understand that from

1 a Government perspective though, all the information
2 that the commercial sector collects, guess what?
3 If the commercial sector has it, the Government
4 might be interested in it so the concerns are across
5 the board. First of all, just to bring the meeting
6 to a close I want to thank the workshop team, my other
7 colleagues, Martha Landersburg, Peter Sand.

8 (APPLAUSE)

9 MODERATOR LEVIN: Rosalind Kennedy, Mike Ryan and
10 Erin Odom who are outside and Earl Crane, our other
11 moderator. I think we've seen the powerful impact of
12 this new media. Obviously in the most recent election
13 of President Obama, but also obviously as important in the
14 last few weeks of what's been occurring in the
15 political developments in Iran, there's no question
16 but we're seeing some huge changes in communication
17 and the Government not surprisingly takes a little
18 while to catch up to these changes in technology.
19 Some of us are old enough, gray enough, to remember the
20 Government trying to deal with Web Gov. 1.0 and the
21 challenges there, and it took us a while to get our
22

1 arms around that. It's going to take us a little
2 while to get our arms around 2.0 but I think hopefully
3 this particular conference has helped to frame the
4 issues a little bit more sharply giving you some more
5 information to go home with about how to consider
6 these issues and most importantly from the perspective
7 of this panel, that you consider the Fair Information
8 Practice Principles as a useful road map to get
9 us to Oregon and space beyond. I think there's
10 a generally agreement that privacy is a core value for
11 Government to protect. The question really in this
12 context is how do we ensure that these new innovations
13 don't erode privacy but rather help us move forward in
14 transparency and collaboration with privacy being
15 addressed. As in the past in our other workshops,
16 we'll prepare a report. We'll try and do this as
17 quickly as we can because we think this information is
18 very valuable now. We'll also produce a transcript.
19 We'll post it on our Web site. And if any of you have
20 comments as a result of what you've heard, if you would like
21 to add comments to the workshop collection that we've
22 already received, please go to our Web site. Comments

1 up until July 10th will be greatly appreciated.

2 So thank you all so much for your attendance.

3 (APPLAUSE)

4 (Where upon workshop concluded at 12:30 p.m.)

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22