THE BROOKINGS INSTITUTION

# A NEW FRAMEWORK FOR CONSUMER DATA PRIVACY PROTECTIONS

Washington, D.C.

Thursday, July 21, 2011

PARTICIPANTS:

**Featured Speakers:**

JON LEIBOWITZ
Chairman, The Federal Trade Commission

CAMERON F. KERRY
General Counsel, U.S. Department of Commerce

**Moderator:**

DARRELL WEST
Vice President and Director, Governance Studies
Director, Center for Technology Innovation
The Brookings Institution

**Panelists:**

ALLAN FRIEDMAN
Fellow and Research Director, Center for Technology Innovation
The Brookings Institution

MARK COOPER
Director of Research, Consumer Federation of America

* * * * *

ANDERSON COURT REPORTING
706 Duke Street, Suite 100
Alexandria, VA 22314
Phone (703) 519-7180 Fax (703) 519-7190

P R O C E E D I N G S

MR. WEST: Good afternoon. I'm Darrell West, vice president of Governance Studies and director of the Center for Technology Innovation at the Brookings Institution and I'd like to welcome you to this forum on privacy.

Privacy, obviously, is one of the top concerns for online consumers. All of us are putting more and more personal information, data, in fact, our entire lives online so people are worried about whether that privacy is maintained and under what conditions. Some of the threats are not new but there are other challenges that are getting more complex. This includes more organized efforts to invade personal privacy. Also, there are new technologies and new practices, such as facial recognition, geolocation, and behavioral advertising that uproot conventional notions of privacy.

To help us deal with this subject the administration has put together an internet policy task force led by the U.S. Department of Commerce. It is articulating a new privacy framework that outlines a set of principles that define rights and obligations regarding personal data and among other things proposes a consumer privacy bill of rights. The Federal Trade Commission has authority to enforce compliance and has its own framework for consumer privacy that emphasizes improved

transparency about data use practices and giving consumers clear choices about how their data will be used.

Today we are honored to have two of the principal leaders in this area who will share their views about ways to protect privacy without endangering technology innovation. Our first speaker is Jon Leibowitz, who is chairman of the Federal Trade Commission. During his tenure as chairman he has focused on stopping scams that prey upon consumers suffering from the economic downturn, preserving competition in health care and blocking anti-competitive patent settlements in the pharmaceutical industry and promoting competition and innovation in the technology sector. Before joining the Commission, he had a long career of public service as well as doing some other things. He was the democratic chief counsel and staff director for the U.S. Senate Anti-Trust Committee from 1997 to 2000. He focused on competition policy and telecommunications matters in that position. He also served as chief counsel and staff director for the Senate Subcommittee on Terrorism and Technology. That was from ’95 to ’96 and the Senate Subcommittee on Juvenile Justice from ’91 to ’94. He also served as vice president for congressional affairs for the Motion Picture Association of America from 2000 to 2004. So please join me in welcoming Jon Leibowitz to Brookings. (Applause)

MR. LEIBOWITZ: Thank you, Darrell, for that kind and

entirely undeserved introduction. I know you've had a busy day doing multiple fora, a multi, multi-stakeholder process. So thank you for that.

It's a pleasure to be here today with my friend Cam Kerry from the Department of Commerce to discuss how together we can advance consumer privacy. And I just want to thank the Brookings Institution for putting this event together, as well as -- and I look around the room and I see so many people in the audience who are committed to privacy, whose companies are committed to privacy, who have worked at the FTC, a truly bipartisan agency who are working at the FTC though not from my office because we really do try to be in a town where there is -- and you can see it -- a lot of partisanship, we really do try to be consensus-driven and collegial and try to come up with really a better consensus-driven -- better consensus-driven products and solutions.

Today, as all of you in the room know, vast amounts of personal information about consumers are collected and used by just a wide array of companies from retailers, advertisers and search engines, to data brokers, lenders, and employers. And there's no doubt that there are real benefits to this data collection. We all enjoy having good interest rates on loans, deals on household items, particularly in tough economic times, even more relevant, advertising. And I think we all enjoy the sort of free access to information that we've now come to expect.

But as the FTC in our report and the Department of

Commerce have explained I think repeatedly in testimony and in reports, the vast majority of consumers simply have no idea that they're purchasing history, their particular financial situation, information about their health and other personal data is sold to data brokers and lead generators, not to mention insurance companies, lenders, and potential employers. Consumers -- and I think that's really all of us in the room today -- really have little understanding -- one might say no idea -- of how this data is collected, how it's sold, how it's used both online and offline. And, you know, you don't have to look too far to see examples of this.

And I don't know if anyone saw the piece earlier in the Washington Post this week about -- I think it was called the Fourth Bureau -- but it was about data collection, data brokers. And so I think there is a fair amount, I think by all of us, by all the stakeholders in this process of concern, and that's one of the reasons we're just absolutely delighted that the Department of Commerce is playing such an active role on privacy.

Now at the FTC, we have had a two-pronged approach to protecting consumer privacy for at least the last four decades. It's enforcement and it's policy work. So on the enforcement side we brought more than 100 spam and spywork cases in the last decade and over 300 cases that relate to the consumer privacy. And we recently entered into a major settlement with Google, as I'm sure you know, relating to the roll out of their Buzz social network.

Privacy policy work has also been a priority at the Commission since the 1970s and today it is really front and center on our agency's agenda. So in December, as most of you know, Commission staff issued a preliminary privacy report that recommended three main principles. First, industry needed to adopt a privacy by design approach to building privacy protections into their products and services at the outset. So an example of where you don't do that is sort of early peer-to-peer. That's why we saw so many data breaches is because what was clearly going on is they've had these cool and interesting technologies. In my previous life when I worked at the Motion Picture Association we thought they were very much privacy enhancing. But putting that aside, what they didn't have -- what they didn't have was real sort of security features. And that's why you saw a lot of confidential information, and still do, leaking out from those early forms of peer-to-peer.

Second, companies should provide and need to provide simpler and more streamlined choices to consumers about their data practices. So choice is a second element and a critically important one. And finally, companies need to make their data practices more transparent for consumers.

Does anyone in this audience read privacy policies on the Internet routinely? Could you raise your hand? I see one -- well, this is a pretty sophisticated audience.

Okay. So I'll just tell you. In preparation for testifying before Congress maybe a month or two ago, I asked folks to look at mobile privacy policies and we found one mobile privacy policy that it took 109 clicks to get through. And so, you know, you don't have to be the head of the -- you don't have to be the secretary of transportation to know that that is a bad privacy policy and you shouldn't be reading it while you're driving.

I'm sorry. That was a joke. And if you're not going to -- you know, I'm not going to do the substance part of this discussion unless you -- fine. (Laughter)

Anyway, so we developed our privacy report with sort of dual purposes in mind. So first, it's intended to be a tool for policymakers, including Congress. In fact, let me reverse this order. First, it's intended to guide sort of industry as it develops, and some of your companies have done this. Effective privacy practices and really best privacy practices and self-regulatory guidelines. So second, it's also intended to be a tool for policymakers, including Congress, as it begins to develop solutions and policies and potential laws governing privacy.

And our draft report, one of the things it does, it really does complement the draft recommendations that the Department of Commerce has made in its Green Paper for protecting consumer privacy. And I think by embracing fair information practice principles and working on a consumer privacy and sort of endorsing a consumer privacy bill of

rights, you know, when was the last -- there have been many Departments of Commerce who cared about privacy regardless of party affiliation, but when was the last time a Commerce Department, or when has a Commerce Department ever endorsed a privacy bill of rights before?

In any event, it seems to me that the Commerce Department is really -- and the work that you're leading, Cam -- you and Larry Strickling -- is really pushing the debate much closer to more meaningful privacy protections for all Americans, as well as -- and I think this is also very important -- certainty for businesses. So as I think you'll discuss in more detail, you proposed or Congress has proposed legislation that could be implemented through enforceable codes, developed through a multi-stakeholder process. This could be a promising way to implement the kinds of protections that the FTC staff propose in its report. And to partner with businesses, in fact, even before the legislation is enacted.

Now, at the FTC we have a fairly long history of supporting multi-stakeholder processes that have led to self-regulation, really going back to the 1990s. In 2007, for example, we held a workshop to examine the privacy implications of online behavioral advertising. The workshop resulted in proposed principles to guide self-regulatory efforts in this area. In turn, industry developed a number of self-regulatory initiatives, including new codes of conduct and online tools to give consumers more control over receipt of targeted advertising. And while these efforts haven't been

fully implemented, they certainly are a positive step or a series of positive -- led to a series of positive steps to better protecting consumers' privacy online.

We did roundtables, and as I look around the room many of you were involved in them in 2009 and 2010. And that was another example of where we tried to bring together different stakeholders. And the roundtables explored really -- some of you were there -- the effectiveness of current privacy approaches and the rapidly evolving market for consumer information. We brought representatives really from all sides of the privacy debate together -- industry, consumer groups, government, academics, and technologists. And the result was what we think was a pretty good draft staff report on privacy that we put out in December 2010.

And this multi-stakeholder process, as some of you know, is ongoing. In response to questions posed by the report, we received I think more than 450 comments -- more than 450 comments from interested parties. We're analyzing those now. We expect to issue a final report later this year.

So let me talk a little bit about moving forward. So the process proposed by the Commerce Department is in an early stage of development and our staffs are still discussing how it's going to work in practice and the respective roles of the agency. But this is a real

opportunity to highlight some of the critical elements that are essential to a fair process and an outcome that ensures both the protection of consumer privacy, as well as business innovation.

I think first we agree strongly with the Department of Commerce that a multi-stakeholder process has to be driven by clear standards. No one benefits if the standards developed are difficult to understand or are difficult to apply or implement. Not businesses, not government, certainly not consumers.

Second, as I think you'll hear from Cam, a transparent process needs to involve sort of all stakeholders. And that's really vital. In our experience, all interested parties need to be at the table, including industry, consumer advocates, as well as other sort of interested parts of government. And everybody needs an opportunity to be heard. We are dealing with very complicated issues here. It is a very fast paced, dynamic world and a plan that doesn't include input from all sides just isn't going to work in the long run.

And third, as I think all of us know, any standards that result from this process have to be enforceable. Consumers and businesses have to know and they will want to know -- all of us in this room want to know -- that the standards that we implement don't just work on paper but have real meaning.

Fourth, again as the Department of Commerce recognizes

and I think they've done just a magnificent job with this whole initiative, both Commerce and the FTC will need to make sure that the privacy standards are strong ones. We have to be confident that this program is going to be effective in protecting privacy and standards that are nonregulatory and easily implemented by businesses are even better. These features are critical and we know that these elements are a core part of your efforts here.

Now, at the FTC, we have had a long history of working together with the Department of Commerce on privacy issues. The U.S.-E.U. Safe Harbor framework and APEC are just two examples of our cooperative privacy efforts. We have consulted with the Commerce Department as it has developed its current privacy recommendations and they have consulted with us. It's really a terrific working relationship where I think we benefit from the interaction overall. Certainly, we do. You might be -- it might move you to a slightly lower level. But I actually think it's a wonderful working relationship and with benefits to both sides.

So we are fortunate that we have people like Cam Kerry and assistant secretary Larry Strickling, who are really dedicated to protecting consumer privacy in a thoughtful and balanced way. And we're also lucky that we have Senator Kerry and I believe Senator McCain involved in legislation. And they are committed as well to finding ways to protect consumer privacy without overly burdening businesses. So I want to

thank you for inviting us here today or inviting me here today to speak and really for helping to move the ball forward on our shared efforts to protect consumer privacy. We at the FTC look forward to working with our friends at the Department of Commerce and really everybody in this room to protect consumer privacy in a meaningful, flexible, self-regulatory way.

Thank you so much and I'll be happy to turn it over to Cameron. Do you come up, Darrell? I'll turn it over to you. I'll go sit down. (Applause)

MR. WEST: Yes. We're going to hear from Cameron Kerry. Then both of them will come up and we'll have some questions and give you a chance to ask questions as well.

Our next speaker is Cameron Kerry, general counsel of the U.S. Department of Commerce. As the general counsel of that department, Cameron Kerry is the principal legal advisor to the secretary. He oversees the work of 325 lawyers in 14 different offices that provide legal advice to the various components facing the department. He is the department's chief ethics officer and serves as chair of the Department of Commerce Privacy Council. During his year as general counsel, Mr. Kerry has engaged in a wide range of issues facing the department. He has been a leader on work across the U.S. Government on patent reform and intellectual property issues, privacy and security. He has traveled to the People's Republic of China several times and serves as a co-lead in the

transparency dialogue with China and the U.S.-China Legal Exchange. Previously he was a partner in the Boston office of Mintz Levin, a national law firm. He has over 30 years of practice as a communications lawyer and has dealt with many issues involving telecommunications, environmental law, privacy, and insurance regulation.

So Cameron Kerry, please come up. (Applause)

MR. KERRY: Well, Darrell, thank you so much. You know, I had to laugh when Jon asked if people read privacy policies. It's a question I often ask. I didn't look back in the room to see how many people raised their hands. I did ask that question of a room full of European data privacy commissioners and their staffs about a month ago and there were maybe 40 people in the room, four or five hands went up. So it's a common problem.

Darrell, I want to thank you for your introduction and for putting this event together. I'm very pleased to be here to talk with you and particularly to team up with -- today with Jon Leibowitz.

You know, in the 1990s, the Department of Commerce worked with the FTC, with the White House, on the framework of Internet policy that's guided e-commerce regulation for the past 10 years. In that time, the leadership, the thought and in policy leadership and enforcement of the FTC, has been a real tribute to the value of independent agencies. As the Commerce Department has re-entered in this space, we've worked

in partnership with Jon, with his colleagues, and with his superb staff.

We found complementary roles, converging viewpoints. The Trade Commission's mandate is consumer protection but, you know, they recognized that consumers benefit from business innovation. Our mandate is to promote foreign and domestic commerce, but business depends on the trust of consumers. It's been very much a guiding principle for our work. I was with Secretary Locke today. We were talking about this work and he said exactly that. That, you know, businesses really need the trust of consumers.

Many of you know that last March the Obama administration announced support of legislation to create a consumer privacy bill of rights, a baseline data privacy protection. We believe that a baseline protection should be flexible, should be enforceable at law, and serve as the basis for the development of enforceable codes of conduct. These codes of conduct should specify how the principles in the bill of rights would apply in specific business context.

So what I want to talk about today is how this multi-stakeholder process can shape the broad principles articulated as consumer rights, as business obligations, and fashion them into enforceable codes of conduct that will specify how the principles apply in particular contexts and provide to -- both to businesses and to consumers the predictability and the certainty that we seek.

The Obama administration believes that flexibility provided by a multi-stakeholder process offers the most effective solution to the challenges that are posed by this fast-changing technological environment, economic environment, and social environment that the Internet has become today. That the digital economy has become as part of our society. We need a process that allows industry to be responsive to changing consumer expectations and enables stake holders to identify privacy risks early in the development of new products and new services. We need a process that is nimble enough to respond quickly to consumer data privacy issues as they emerge and that can address them without the need for legislation or regulation because legislation and regulation simply do not move at Internet speed.

Multi-stakeholder processes of the sort that we are talking about are not an untested idea. Groups like the Internet Engineering Task Force, the Worldwide Web Consortium, have used transparent, consensus-driven processes to set a wide range of Internet technical standards. The processes have been successful in part because stakeholders share an interest in solving the underlying challenges. Today, the standards for basic Internet communication standards that support trillions of dollars of economic exchange over the Internet today have been developed through these consensus-driven, network-like processes.

The 1990's Internet framework that I mentioned began with a series of multi-stakeholder events and forums that informed policy and prompted self-regulatory action. Major websites agreed to post privacy policies. The nascent online advertising industry developed a code of conduct and importantly, the FTC enforced compliance with these voluntary standards. The FTC's current work on "do not track" carries on this model. I applaud Jon Leibowitz and the FTC, as well as browser developers, for -- and privacy advocates and others for the work that they've done to provide options for greater control over personal information.

So two key characteristics of a multi-stakeholder process for a wide variety of challenges, including data security, including "do not track," are legitimacy and flexibility. Legitimacy means that a broad array of stakeholders have a chance to be heard and actually are heard. The process we envision will put industry leaders at the table alongside consumers, privacy advocates, state regulators, academics, among others. We want to engage all of them in a dialogue about how to guarantee the privacy that consumers have a right to expect, while enabling businesses to develop new technologies, products, and services, while preserving the benefits of these new technologies that Jon alluded to at the beginning of his remarks.

Flexibility means that the process must be adaptable to

innovation and to changes in technology and services. Issues in the digital economy will touch on technology, business needs, individual values, U.S. law, foreign law, and policy, among many other issues. The process needs to be able to accommodate all of these different, sometimes converging, sometimes competing considerations.

So what will the federal government's role be in this process? As I said in the Green Paper that we issued last December, more than self-regulation is needed. At this point, it's clear that an effective and a representative process usually -- not always but usually -- takes a nudge from the government. That's why we see a need for the government to take the initiative in convening stakeholder discussions. We believe that the executive branch involvement as a facilitator will inject energy, legitimacy, and urgency to get stakeholders moving, to get the process of developing enforceable codes under way.

Let me say a little what the federal government will not do as part of this process. The federal government will not be a gatekeeper that decides who can participate. Federal government will not hold the pen in the writing of codes of conduct. The federal government will not force anyone in the private sector to adopt them. The federal government also is not the only viable convener. If trade associations, consumer groups, companies, others step forward without any nudging, they're welcome. Let 1,000 flowers bloom.

So how do we begin? The Department of Commerce would initiate the process by working with private sector, stakeholders, with consumer groups, privacy advocates, government partners, to identify specific areas where privacy practices are unclear and where clear rules would benefit consumers and benefit businesses. The end goal here is to produce an enforceable code of conduct that will receive approval by the FTC.

In keeping with the Obama administration's commitment to transparency and openness, we'll make the process visible and accessible to all. Participation will be open to anyone who's interested in defining a code of conduct and willing to work hard to develop a consensus around a code of conduct. We'll ask participants to submit written positions, to answer specific questions, to draft potential codes of conduct in advance so that meeting attendees and remote viewers can grapple with the difficult issues it will take to reach consensus.

The Department of Commerce will enlist stakeholder participation by issuing public notices that describe the issues in play and announcing times, dates, and places for public meetings, and will provide opportunities for remote participation by live streaming and options for viewers around the world to post reactions and comments. We intend to run an open process but independent -- industry stakeholders and independent third parties will hold the pen in drafting the codes.

The Federal Trade Commission's role in this process is essential. So I'm especially pleased to be joining Jon Leibowitz today. We believe that effective enforcement will benefit from legislation that grants the FTC a clear authority in the commercial data privacy arena. Granting the FTC explicit authority in enforcing the principles of the bill of rights -- privacy bill of rights -- will strengthen its role in consumer data privacy policy and give it the enforcement tools that are needed in this field. And if companies know that the FTC can enforce baseline legislation, that is an incentive to define codes of conduct and to move forward with the process as this world advances into new areas.

So under our proposal the Federal Trade Commission would be an active partner and participant in the multi-stakeholder process. We look forward to the FTC's voice and expertise from the beginning of the discussion. And at the end of the discussion it would be the FTC's job to determine if a code of conduct sufficiently implements the requirements of the statutory bill of rights. Simply promising to abide by a code of conduct is not enough.

At the Department of Commerce, we don't intend to wait for legislation. We are going to begin to identify pressing privacy issues that can benefit from a multi-stakeholder process and we'll continue discussions with the FTC about baseline protections, about how to approve codes of conduct and about how to implement the multi-

stakeholder process. And then we will begin to convene groups to energize this process in a conversation that today is long overdue.

So I want to ask all of you to join us in that conversation. The innovators of the digital world have created great opportunities -- economic opportunities, social opportunities -- none of us imagined 10, 15, 20 years ago could exist. But for the Internet to continue as a place of innovation, as a place of economic opportunity, it also must be a place where consumers, individuals, feel safe, where the deeply held values of privacy are protected.

So I want to thank Darrell West, Mark Cooper, for joining us on this program later today. They are some of the kinds of voices that need to be part of this discussion. Most of you are stakeholders who need to be part of this discussion to help develop clear, enforceable codes that will give clear instructions to industry, give confidence to consumers. So we need your participation. We need your best thinking. These won't be easy conversations but -- and there won't be easy consensus. But without you this multi-stakeholder process cannot work.

So I thank you for being here and I look forward to continuing the conversation. Thank you all. (Applause)

MR. WEST: Okay. I'm giving him a minute to turn on. I guess the mike is on now. So first of all, Jon --

SPEAKER: It's on for you.

MR. WEST: Yours will be on shortly.

So thank you very much to each of you for your comments.

I'll start with one or two questions and then we'll give you a chance to ask about your issues as well.

One aspect of privacy concerns data breaches, and certainly just in recent weeks we've seen companies that have experienced data breaches, sometimes it's been weeks or longer before they actually notified consumers who were affected by this. So one question I'd like to ask each of you is what is the proper timeframe that companies should use to notify consumers who are affected by data breaches? And then the second aspect is right now companies are required to notify but generally that is governed by state law, and of course there are different laws across the country. Some people suggested the need to harmonize the laws at the national level and you get into issues of some states having tougher rules and other states having more relaxed rules. So I ask each of you to respond to those questions.

MR. LEIBOWITZ: Sure. Well, one of the proposals that we made is there should be national data breach legislation. That is now part of the administration's cybersecurity bill. I think the wave of data privacy breaches that we've seen over recent weeks, recent months, are a real wake-up call to get that legislation passed, to create one set of expectations and requirements. There's no question that the array of

state data privacy breach of laws has been a tremendous driver in advancing privacy and advancing the professionalization of privacy. We need to make that national.

MR. KERRY: Yeah. And I think as a general matter we agree. We probably -- we have brought under Section 5, Unfair Deceptive Acts or Privacies authority more than 30 data security cases. We have supported certain iterations of data security legislation in the past and the states have been drivers of notification and I think different states have different standards. It's generally notify in a reasonable amount of time or with some alacrity or in-between there literally -- when I came to the Commission I think a handful of states had data notification breach and now it's 46.

SPEAKER: Now it's 46.

MR. KERRY: And now it's 46. So, so you can see the growth of that. But I think Cam is absolutely right. You don't want a crazy quilt patchwork of statutes, even if most of them or the vast majority of them are reasonable. You know, if you get the right -- if you get the right standards in a federal law, ones that protect privacy and insured notification, then that's generally preferable.

MR. WEST: What about privacy rules on mobile devices? We now see apps that access user phone numbers, e-mail contacts, call logs, and Internet data. How should we be integrating mobile privacy into

the more general approach to privacy? And should there be a no more track for mobile devices?

MR. LEIBOWITZ: Well speaking, well, I think the Commission, and again, we're very consensus-driven, is very interested in ensuring that privacy protections do extend to mobile devices. We talked about that in our report. Commissioners talk all the time and this is an area where we're very concerned about. And of course, our statute applies to mobile devices as well. You can't engage in an unfair deceptive act or practice no matter what the platform is. In terms of -- I guess I'd say in terms of going forward it's an area we're going to continue to concentrate on and think about and of course, you know, the sort of one thing you want to ensure is that standards shouldn't be different depending on the device. They ought to be uniform and they ought to be -- and they ought to ensure people's privacy. And so much commerce, as everyone in this room knows, is moving, you know, to mobile platform.

MR. KERRY: Certainly the paradigm for the discussion has been the online world. But what's important about data in this world today is not whether it's mobile or it's online or it resides someplace else but it's in digital form that's easily transmitted by any of these means. So you really need to treat all data alike whether -- regardless of the medium.

MR. LEIBOWITZ: And I think this is really -- going back to the stakeholder process -- I think this is part of the real promise of the

stakeholder process is you can bring together people who are, you know, very involved in the mobile world, for example, and they can help to design in theory sort of good, robust privacy protections.

MR. KERRY: But, you know, part of what we're thinking about is that really how data is treated becomes a function of the context, the relationship with the consumer. I mean, for example, the FTC's report suggested that certain kinds of, you know, when you're doing an online transaction notice and choice requirements don't apply because they're pretty obviously implied to people. That's part of the context. It's part of the relationship that that customer is entered into with that vendor. We need to carry forward that kind of context, sensitive treatment of privacy across the board.

MR. WEST: Okay. Why don't we move to the audience. If you have a question, raise your hand. We have a question here in the second row. We have microphones that are coming up, so if you could give us your name and if you're with an organization. And we would ask you to keep your questions brief just so we can get to as many people as possible.

MR. SOGHOIAN: My name is Chris Soghoian. I'm a fellow at the Center for Applied Cybersecurity Research at Indiana University. My question is to Chairman Leibowitz.

And so with all the stuff we've been hearing about the

Murdoch scandal in the U.K., there's obviously a lot of attention now on mobile phone and voice mail security. Now, the papers in the U.K. were hacking into voice mail in one specific way but here in the U.S. we have our own voice mail security issues. And in fact, three of the four major carriers don't require pins when you're calling from your own number, and there are many off-the-shelf tools that let you spoof your caller ID and break into someone else's voicemail. In fact, Paris Hilton did it to Lindsay Lohan just four years ago. Now, all of the carriers offer consumers an option to require a pin and they advise consumers to set this option but they don't do it for them. So they're not, in fact, using privacy by design as you suggested.

So I have two quick questions.

MR. LEIBOWITZ: Yes.

MR. SOGHOIAN: One, should they in fact be requiring pins in all cases and following privacy by design? And two, do you think the FTC has the authority in the space with regard to voicemail security as a common carrier service or do you have authority in this space?

MR. LEIBOWITZ: That's a great -- those are two great questions. So the answer to the first question is yes, we think they should engage in privacy by design. We like to think that most companies are moving in that direction or sophisticated companies are there already. Two is we have no jurisdiction whatsoever because we cannot do

anything. We have no jurisdiction over common carriers and we have long -- on a bipartisan basis we have long supported eliminating the common carrier restriction but -- or exemption from our jurisdiction but it's there now. It will be there for the foreseeable future, although some people were talking even in the industry about removing it in the privacy context. So good question. Wish we had some authority there. Agree with the premise.

MR. WEST: Okay. Other questions? There's a question over there.

MR. LEIBOWITZ: From Peter Swire, professor.

MR. WEST: Actually, there's a microphone coming up to you -- right behind you.

MR. SWIRE: Thank you. Ohio State University and various organizations.

My question is especially for Cam Kerry as general counsel of the agency talking about some of the procedural rules that apply to federal agencies when they try to reach out to multi-stakeholders. So there's the Federal Advisory Committee Act, there's the government Sunshine Act. And then if you have meetings with people there's a question of whether the Freedom of Information Act and Deliberative Process would apply. In other words, whether the contents of those meetings would then be FOIA-able basically for everybody. As general

counsel, have you had some thoughts about how these sometimes fairly directive federal statutes apply to the multi-stakeholders (inaudible)?

MR. KERRY: Yes. We certainly looked at the question whether the Federal Advisory Committee Act applies to the kind of stakeholder discussions that we're talking about. And the answer is not because ultimately the federal decision process is a decision by the FTC that would follow on from that -- from those discussions.

MR. LEIBOWITZ: I'm sure if I had our general counsel here he would agree with Cam, who is a terrific general counsel. And I'll just leave it at that. Except to say going back to some of those rules, the Sunshine Act and FOIA, because most of our FOIA requests are from competitors seeking an advantage over or companies seeking competitive advantage over their rivals, it might at some point be a good idea for Congress to sort of look at whether, you know, 20 and 30 years after these well intentioned, and I think in many ways very good laws were written. Some as close to 40 years actually. It might be a good idea to just go back and just do a little sort of reg review on them I would say to see whether the right balance is still being struck.

MR. WEST: There's a question right here in the fourth row. Yep, right there.

SPEAKER: Thank you. First I want to thank both Cam Kerry and Jon Leibowitz for their leadership and the agency's focus and

the administration's focus on the issue of privacy. I think this is unprecedented and it's very much appreciated. But I do want to go back to what Peter Swire was saying about the stakeholder process.

A couple of issues. One, you're right. Consumer trust is going to be very important but you're going to also have stakeholder across the board trust in this process. And part of trust is transparency. And if there's no mechanism for ensuring transparency in this decision-making process, which will be fed into the FTC which will allow transparency because of its mandate and it is a federal government agency, I think that's going to be problematic.

The other issue is defining stakeholders. In our experience in the U.S., stakeholders tend to, and sometimes especially if the advocacy community versus the non-profit or for-profit entities may not be that comfortable with each other and you're talking about a very diplomatic process when you acknowledge their points of agreement, points of disagreement, and how you resolve that.

So I do think what Jon said about standards is very important and I wanted to find out how do we get there because, of course, the Department of Commerce has one of the best standards development agencies in the world at NIST. So we do want to see as advocacy organizations a very fixed, defined process and definitions that will guide or at least give us some fixity about what's going to happen in

the long term.

MR. KERRY: Yeah, I mean, the NIST -- the NIST model is very much a part of my answer. Look to as the model the NIST standards development or the work that I mentioned, for example, the Internet Engineering Task Force. Those are very much transparent processes where the ongoing work is available on websites, not just for the parties sitting at the table to see but for other people to see and communicate on. So, you know, I think those -- that's a critical piece of it.

I said that these are going to be difficult conversations. Certainly, the effort would be to have stakeholders come to a consensus but I think we recognize that's not going to happen all the time. It would certainly be open I said as well. You know, this doesn't have to be something that we convene or that the FTC convenes. It can be convened by private sector stakeholders. I think that also mentions the possibility that somebody would say the Internet Advertising Bureau could develop a set of behavioral advertising codes and come to the FTC and say, look, we want you to bless these as sufficient and enforceable without government involvement and without necessarily agreement by other stakeholders. You get to decide whether that's enough or whether objections that other people may raise should prevail.

MR. LEIBOWITZ: Right. If they came to us we would like to see no tracking as opposed to just no advertising back to consumers but

anyway that's for another time. But hopefully in the not too distant future. Go ahead.

MR. WEST: Okay. Right here is a question.

MR. SZABOW: Carl Szabow from NetChoice. This is actually for Mr. Kerry and Chairman Leibowitz. It's with regard to what you both said about one of the main concerns is scaring away consumers from the Internet. If they don't know what's going on they might go in the other direction but you've got LinkedIn that has 1.3 million subscribers a month. You have Twitter that has 300,000 new subscribers a day. And then you've got companies like Google who have a kind of dubious history with privacy. They just launched their Google+ and they're seeing a million people sign up a day. So I know Commissioner Rush has asked about this. What evidence have you all found that people are actually seeing these privacy concerns and going in the opposite direction and running away from the Internet?

MR. LEIBOWITZ: I think we have said at our commission that people are running away from the Internet but I think it is pretty clear if you look at consumer research there's been some polling data that -- and you talk to people who are stakeholders -- that there is a concern, I think. And you look at things like, you know, and it ranges from the potential for data breaches through the Internet which have been, as we know, all too common, to the lack of control of people's information by third parties with

whom they have no relationship to. And I think there's -- so the question isn't, you know, has it scared people off from the Internet. The Internet is growing and thriving. You could ask -- you could say, well, you could say, well, would there have been sort of more involvement I suppose if there hadn't been these breaches? I suspect there would have been. But the question is really, you know, are consumers concerned about privacy on the Internet? Yes. The vast majority are. And is the concern legitimate? And I think most of us would agree it is.

So of course the Internet is growing. We love that. It's a good thing for commerce. It's a good thing for people's social interaction. You described, I think, the ways in which many Internet companies have grown and that's a good thing. We just want to make sure it grows with privacy protections and hopefully in a flexible, self-regulatory way.

MR. KERRY: Yeah. That's actually right. This is a vital economic driver. It's vital to our economic growth. If you look at the growth that we've had over the last few years, you know, the digital economy, the e-commerce sectors have been way ahead of the traditional economy. This is vital for our continued economic growth. It's vital for key components of the U.S. economy where we have real competitive advantages. But, you know, the data that Jon alluded to shows that when it comes to adopting cloud computing, the single greatest concern that people have is security and privacy. You know, we're facing in that world

the sort of situation that we had with e-commerce 15 years ago where, you know, the key hurdle was getting people to accept online credit card transactions.

So this is important for that reason and I told some people here this story before but I was at a policy forum a couple of years ago that was a mixture of academics, government, business, you know, NGOs across the political spectrum. We had this assignment to look at different scenarios for positive development of the broadband world and for negative development. Each of these folks went off independently and looked at these scenarios, looked at key drivers, key risks for development. Every single one of them came back and reported the same key driver, the same key risk, and every single one of them articulated it independently in the same terms -- trust. I take that message is this is key, you know, a key issue for a key part of our economy.

MR. WEST: Okay. We are out of time for this component. We have a couple of experts who are going to come up and we're going to continue our discussion about privacy but I want to thank Jon Leibowitz and Cameron Kerry for sharing your views and good luck with your efforts. And we hope you come back.

MR. LEIBOWITZ: Thank you.

MR. KERRY: Thank you all. (Applause)

MR. WEST: So I'm going to ask Mark Cooper and Allan

Friedman to come up and we will continue our discussion of privacy.

Okay. We're going to continue our discussion of privacy issues with Mark Cooper, director of research of the Consumer Federation of America and Allan Friedman, my colleague who is a fellow in governance studies here at Brookings.

Mark holds a Ph.D. from Yale University. He is director of research at the Consumer Federation of America where he has responsibility for analysis and advocacy in the areas of telecommunications, media, digital rights, economic and energy policy. He's provided expert testimony in over 250 cases. He's written a number of different books, including *Media Ownership and Democracy in the Digital Information Age*.

Allan Friedman is a fellow in governance studies at Brookings and also is research director for the Center for Technology Innovation at Brookings. His work spans the social sciences, public policy, and computer science. He's written extensively on various aspects of technology innovation, including a paper on cybersecurity that he just released this morning. So any of you who are interested in seeing that you can go to our website, brookings.edu.

So I want to start with Mark. How do you think we should approach the privacy issue and what is the role of government in overseeing this area?

MR. COOPER: The fascinating thing to me about the previous discussion is the tremendous desire to talk about self-regulation. We talk about robust, enforceable self-regulation. And point of fact, they're not talking about self-regulation at all. I understand the PR value of that but if you think about it they talked about statutorily defined rights, enforceable baseline legislation, approval by the FTC, public notice and comment after the multi-stakeholder process. Those characteristics are not self-regulation. They are, in fact, regulation. Now, it may be a little bit more flexible, enforcement may be shifted, but the desire to appease the business interests with the word self-regulation needs to be balanced, I believe, by a need to appease the public interest with the understanding that there is really regulation there.

And the interesting thing to me is that as you heard these two leaders in this field speak, they are actually talking about a real regulatory regime and they fail to get that message across. And to me that's really a tragic mistake because this is not a debate about self-regulation versus command and control regulation. This is a debate about something in between. And if you look at the literature, people talk about enforceable self-regulation, social regulation, mandatory self-regulation. They've got all these adjectives. It's not self-regulation and we really do need to get beyond that.

Having moved beyond that there's no doubt, I believe, that

traditional command and control regulation will not work in this space for many of the reasons they spoke about. It is too dynamic, too rapidly moving. The consumer demand is too diverse to have a very rigid set of command and control rules so we need this flexible process. We need to have a good multi-stakeholder process. And Cam Kerry listed all the key characteristics of a good multi-stakeholder process. They were all there -- inclusiveness, representativeness, coverage, transparency. All of those things. So we are not talking about something that won't work. It's something that can work.

The one thing that I don't hear and I really want to hear is participatory enforcement. Writing the rules under what you live is a good part of democracy but enforcing those rules by having the public directly involved in the enforcement process I think is something that we need to think more about. We need to institutionalize crowd sourcing and I think I said that six months ago here at Brookings. I'll have a *Law Review* article out soon that's describing that. We need to get the public directly involved in the enforcement of the rules because frankly the central bureaucratic government can't do it. It cannot possibly police this space. We have to find ways to get the public involved.

So from my point of view very encouraging. I mean, we are now talking about a regulatory regime that engages the public based on legislation and principles and law. We're not talking about self-regulation

anymore. I understand their need to say that but we're really not talking about pure self-regulation anymore.

MR. WEST: Okay. Thank you.

Allan, you have written and thought about the economics privacy. Could you explain a little bit about what you mean by that and what are the incentives that the various stakeholders actually have in the privacy area?

MR. COOPER: So I think focusing on the economics of privacy allows us to sort of take a bunch of multi-dimensional values and try to at least come up with a way of condensing them to better support the policy analysis process. And there are a couple of interesting tradeoffs that we can begin to focus on that I think raise further questions.

So one is this idea of opting as a model that's been promoted by both the FTC and Commerce in cases where we're dealing with a lot of very important data. And the interesting question there is how do we define what a transaction is? On one hand we can say, listen, anytime you have a negotiation whereas you can't come in here unless you give me data, you can't participate in what we have here unless there is data offered, you can make the claim that that is not really informed. That is not perfect consent. That's not unambiguous consent.

The problem with the logical extreme of this position is now there's no such thing as a two-way transaction that involves personal data.

The only time you can ask someone for their personal data is if you give them nothing in exchange for it, which is a strange equilibrium to find yourself at. The flipside is to make explicit tradeoffs for entry in terms of data. So instead of having a pay wall we now have a data wall. This is an interesting model for sort of motivating publishing in the future but I think it falls back on this idea of trying to have very explicit boundaries of where we're going to have this wall and it needs to be explicit.

The second approach for this is how do we incentivize privacy enhancing technologies and privacy enhancing practices? In the research community there's a growing number of tools that allow people to gain value from data at minimal risk of disclosure, at minimal risk of future misuse, and with the maximum amount of guarantees that you can make to someone that say, listen, bad things won't happen to you. Here's what we want and here's why we can credibly assert that we're not taking anything else because the data sitting over here, we're extracting a certain value. We have those technologies and more and more of them are coming out every day. How can we promote their use? How can we really say let's promote data minimization?

The final question that I think the economics of privacy raises is on the question of behavioral economics. At what point are we interested in promoting policies and practices that make people feel good about privacy but if you sit down as an information scientist and start to

examine what's going on there's not really much of a change. And is this something that we want to try to promote or discourage or be agnostic about?

So, for example, there was a recent study that came out about Facebook data controls. Now, Facebook data controls have nothing to do with the amount of data that the advertisers get from you or what they can do. They're completely neutral with respect to advertising data but they did allow people to have a sense of control. And a recent study by an MIT professor found out that, in fact, uptake on advertisements that were explicitly personalized had -- they had a greater hit rate after these privacy controls were enabled. People had the sense of control even though it didn't give them anything. And one thing we know from behavioral research is, listen, it's not always about actually promoting value. Sometimes you just need to have some value.

If we go back to both the chair and Commissioner Leibowitz and Cam Kerry's definitions, the important thing here is trust. Now, if we can gain trust without improving privacy, are we okay with that? And I think that's a fascinating question that is going to have to be resolved politically.

MR. WEST: Okay. Thank you very much. Let's open the floor to questions from the audience. So again, give us your name and your affiliation. Actually, in the very back there's a question.

SPEAKER: (inaudible) from the Senate Commerce Committee. A few days ago I attended a roundtable -- transatlantic roundtable on privacy and data security. And while the entire panel came forward agreeing with data security, there was no consensus on privacy because Europe had a lot of objections to the privacy bill proposed by America saying that the Patriot Act exposes some flaws. And they had specific complaints against the U.S. wanting to shut down sits outside America saying that that would start something pretty bad. So what are your thoughts on that?

MR. FRIEDMAN: Well, the interesting for me to think about in the U.S.-Europe conversation is we're starting from different places and one of the things about America -- and look, I believe privacy is a right. Consumers and public interest advocates have argued it's not an economic good for which I should have to measure the harm but is a right in my belief. On the other hand, I live in America and I have to govern the country I live in. Right? And if you look back historically no major sector of the American economy has ever been subject to regulation unless there was a consensus that there existed a pervasive market failure. I wish it were otherwise but I live here and that's the standard we have used in America. And you go back to the Progressive Era, the New Deal, or the New Society, right, where we had three periods of massive progressive legislation. There was, in fact, an agreement about market failure. It had

nothing to do with rights. A little bit but not a lot.

So you've had this divide between Europe and the U.S. in terms of how they view the problem. I view the movement in the U.S. as the opportunity to close that distance because now we have two agencies that have declared market failure. Now, it's going to be a while before that becomes a consensus but they declared market failure. So today we are beginning a conversation in which the two parties can actually exchange views. Until we had this gap closed we were unable to do so. So from my point of view the U.S. position will, in my opinion, evolve toward the European position because now we're finally talking a language that says we need government action. Until now we've denied the fact that we needed government action. The question will be is there a place we can get together? The recent OECD communiqué had a lot of good stuff in it and some very bothersome stuff in it. Right? But that document reflects less difference between the two sides, I think, than has existed for a decade. So from my point of view this is the start of that process of seeing if we can come to a real global framework that is -- and every negotiation is an exchange of values.

MR. WEST: Right there is a question. If we can get a microphone over here. The gentleman in the blue shirt.

MR. BRENNER: Thanks. I'm Dan Brenner with Hogan Lovells. I appreciated your remarks because this is -- we're launching

kind of a new process that Cam Kerry described in which he says the government will not hold the pen. He said that a number of times. He said he wants the parties to try to dicker to consensus. This is a strange month to be in favor of a consensus-driven Washington but be that as it may. And there are economic differences among say the ISP community and the Google and Search and Facebook community where they view themselves in some ways as competitors. So it's not clear to me that consensus will be easy for those parties to reach because someone may be eating someone else's lunch or part of their dinner if consensus -- if a result comes one way or the other.

So I'm sort of asking both of you how if Cam Kerry says the government is not going to regulate and the FTC doesn't really have rule-making authority but could adopt, I guess, some consensus-driven self-regulatory code coming out of this, how will this actually work in your mind? What would be the best way for it to work?

MR. WEST: Or will it work?

MR. LEIBOWITZ: Well, but let's be clear. He said they wouldn't hold the pen but they did both say -- talk about FTC approval. They talked about statutory bill of rights. They talked about enforceable baseline legislation. Cam Kerry talked about how people could make proposals. He talked about public notice and comment. So there's a lot of the old process in there. And then the question becomes what's the

purpose of change? What are they doing to change the process? And here I think there's something to be had in the sense that you're right. If you put all those industry folks and all the public -- on the public interest side we don't all agree either as you well know -- in a room, you're not going to get consensus. Right? But what you may get is majority reports and minority objections.

And one of the things that I've been interested in in thinking about this, so this is just advisory in a certain sense because ultimately the FTC is going to have to approve it. One of the things we have done in legislation in a number of fields is maybe we take that process and give it a special status in the notice and comment period. This happened with the '96 Telecomm Act. Right? Where the Justice Department Comments to the FCC and they're supposed to be given special deference. Okay? So maybe we do that. Now that all of a sudden gets everybody in the room. Right? Now you've got an incentive to participate because, hey, what comes out of this process will carry extra weight at the deciding body. So there are ways to structure this but I think they realize there is no necessary consensus.

One of the other things that may happen, of course, is that people may agree on what we don't want to do. Sometimes it's a lot easier to agree on things that really don't make sense for any of his, while we can agree on what we should do. So, I mean, for me that process is --

it can play an important role especially where there's such contentious issues. And, you know, he points to the IETF but there's no government standing behind the IETF anywhere. So, and that's not what he's talking about here. So I think it's a process that I believe can contribute to making the regulatory process work a little better, particularly if you can sort of eliminate things that just don't make any sense and as long as there's a backstop. And they're very clear. They don't believe that what comes out of that multi-stakeholder process does not become the law of the land without getting approval from the FTC.

So the industry guys have to figure out is there anything in it for them more than I have to figure out is there anything in it for me. And that's different from what people thought they were talking about six months ago, I think.

MR. COOPER: It's interesting to compare this to something that's similar in sort of the consensus-driven process behind NSTIC -- National Strategy for Trusted Identities in Cyberspace -- having gone to a few of their early meetings to build a similar process. There I think the push behind stakeholders is, you know, slowly nudging towards my paradigm or your paradigm or my business' best model. Here I think the navigation is the inverse of that, trying not to get our business model gored. And I think there are some -- divided into three steps. First, there's the, you know, let's go after the bad -- find and punish the bad actors.

That we can do in a fairly straightforward fashion. You just hold up the worst case -- instead of best practices you have worst practices. I like the idea of participatory enforcement and it can happen even at this early stage. For example, we just heard a report from Stanford saying that there are ad networks that are clicking -- that are using an attack against CSS to find your web browsing history. I could probably agree that that's something that should go in and say it's bad.

Second is this idea of keeping honest people honest. And this I think is actually a fairly limited model. Mechanisms for what happens, say what you're going to do and then do it. I think the hardest part is to resist or to decide whether or not to resist the evolution of not just the technology but the evolution of the marketplace in different directions. Usually in most industries best practices is an ever ascending model. So in information security, best practices today are much better than they were two years ago which are much better than they were four years ago.

It's unclear whether we see that in the privacy space of what the best practice is now. We allow a lot more as business models shift. I think that's going to be one of the key political questions just as a philosophical approach. Are we going to allow flexible business models?

MR. FRIEDMAN: I want to do one thing. Now, one of the reasons I say I believe in this stuff is Consumer Federation participates it

in the environmental space. We have just signed the regulatory negotiation with all the environmental groups and all the appliance manufacturers to increase the energy efficiency of a dozen appliances by an average of about 25 percent. And that was a negotiation and you would never have thought you could have gotten consensus and we then moved that to the Department of Energy which then issues it as a proposed rule. And because it's the result of this consensus process it gets a much more rapid treatment. Of course, Congress immediately produces a bill to say don't do it but that's not -- that doesn't matter because this is now an executive branch decision.

So I would argue that -- and the people who do financial services for CFA say the FINRA approach of a so-called self-regulation works really well. So there are models out there for complex topics that it really can work. And I would encourage people in this room to look for the model that they like and bring it forward. But remember, it's not just plain old command and control regulation. It's something in between.

MR. WEST: Okay. Let's get another question. Did you have a question right here?

MR. DELBIANCO: Thank you. Steve DelBianco with NetChoice.

Mark, I thought your answer on the market failure suffered from the same flaw that Commissioner Leibowitz and Cam Kerry used

when they used this gentleman's question about where's the harm. And here's the flaw. I think that you're conflating, on purpose, data security and privacy -- the breach problem being conflated with the privacy problem. And you're relying upon that to suggest that there's a market failure. It's like saying that because bad guys keep breaking into cars and stealing stuff that there must be a market failure in the market for automobiles. And I don't think the problems can be solved in parallel and I don't think conflating them is really going to get us the consensus solutions we're looking for. Do you think they belong together or are they separate?

MR. FRIEDMAN: Well, see, I would have given a different answer to this trust question because trust is like a nuclear reactor. Right? Once you lose it, it destroys the landscape. And so you talk about privacy by design. The nuclear industry talks about defense in depth. And the answer is that maybe you can't -- don't have the luxury of waiting until you have a nuclear disaster to then say, oh, boy, we had a market failure problem and now let's fix it because you can't repair it. Okay? So one thing is that that level of disaster is something you really want to prevent. And then Leibowitz gives you the data that boy, if that happened we would have a barren landscape. So his job is to make sure that reactor can keep running and not have that accident. So that's one level of answer.

The second level of answer I that now you're asking me to prove the negative. How much faster would the Internet have grown if I had better trust? Well, I will guarantee you that when the Sherman Act was passed and the Interstate Commerce Act was passed and the Federal Trade Act was passed the economy was growing. And the same answer would have been, look it's growing fast enough. What do I need these consumer protections for?

So one, you really can't have the disaster. And two, you can't make me prove the negative. I've got good evidence that consumers are uncomfortable, that they don't do the things you say they should do, that the self-regulators don't comply with their own regulations, the Stanford Study, so I've got all these indications of perverse incentives, asymmetric information, ill-informed consumers, ill-equipped consumers. So there's good evidence that the market isn't working well, could be made to work better, and I really can't risk the disaster.

MR. COOPER: I just want to point out quickly that you are welcome to, as everyone does every three years, have the debate about why do we want privacy in general. People have been having this since, you know, the '74 Privacy Act on forward. That's always a fun discussion to have. The problem is we have it every three years and it usually gets resolved of, gosh, maybe for a variety of reasons privacy is a good idea. There are many, many books about this.

I think the example the gentleman used was astounding flawed for one particular reason. If you look at why people shifted over to a new social network, one of the key selling attributes is that it allowed far better control of personal data and far better privacy protection in one dimension than anything that was currently on the market or had been on the market after eight years of social networks. So the fact that it took that long and several academic papers which led to it I think illustrates that there is still some latent demand.

MR. WEST: Okay. We are out of time. I know there are additional questions. Sorry about that. But I want to thank Mark Cooper and Allan Friedman for sharing their views with us. And thank you very much for coming out. (Applause)

* * * * *

CERTIFICATE OF NOTARY PUBLIC

I, Carleton J. Anderson, III do hereby certify that the forgoing electronic file when originally transmitted was reduced to text at my direction; that said transcript is a true record of the proceedings therein referenced; that I am neither counsel for, related to, nor employed by any of the parties to the action in which these proceedings were taken; and, furthermore, that I am neither a relative or employee of any attorney or counsel employed by the parties hereto, nor financially or otherwise interested in the outcome of this action.

/s/Carleton J. Anderson, III

Notary Public in and for the Commonwealth of Virginia

Commission No. 351998

Expires: November 30, 2012