

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25

FEDERAL TRADE COMMISSION

EXPLORING PRIVACY

SECOND ROUNDTABLE on

EXPLORING PRIVACY

Thursday, January 28, 2010

8:35 a.m.

Cohosted by the Federal Trade Commission and the

Berkeley Center for Law and Technology

University of California, Berkeley

University of California

Boalt Hall, Booth Auditorium

Berkeley, California

## I N D E X

1		
2		Page
3	Welcome by Professor Deirdre Mulligan	3
4		
5	Introductory Remarks by	
6	Commissioner Pamela Jones Harbour	7
7		
8	Setting the Stage, by Director David Vladeck	14
9		
10	Panel 1: Technology and Privacy	20
11		
12	Panel 2: Privacy Implications of	
13	Social Networking and Other Platform Providers	83
14		
15	Remarks, Daniel J. Weitzner, Associate Administrator	
16	for Policy, National Telecommunications and	
17	Information Administration, Department of Commerce	137
18		
19	Panel 3: Privacy Implications of Cloud Computing	145
20		
21	Panel 4: Privacy Implications of Mobile Computing	195
22		
23	Panel 5: Technology and Policy	242
24		
25	Closing by Assistant Director Christopher N. Olsen	289

## 1 PROCEEDINGS

2 - - - - -

3 DIRECTOR OLSEN: Folks, we are going to start  
4 in a few minutes. So if everyone could get settled and  
5 take your seats.

6 All right. Why don't we get started? I want  
7 to thank everyone for coming today. It's a terrific  
8 turnout. We're very pleased to be here on the West  
9 Coast.

10 I'm not going to do lengthy introductions, but  
11 I will say that we are very pleased to have Deirdre  
12 Mulligan, Assistant Professor at the University of  
13 California Berkeley School of Information, welcome us  
14 here today to kick off our second Privacy Roundtable  
15 Event. Deirdre, thank you.

16 (Applause.)

17 PROFESSOR MULLIGAN: Thank you. All right.  
18 Good morning. On behalf of the Berkeley Center  
19 for Law and Technology and the Berkeley campus more  
20 broadly, it is an absolute pleasure to welcome the  
21 privacy community to Boalt Hall. It's an honor, in  
22 particular, to host this second of three Privacy  
23 Roundtables on behalf of the FTC because of its strong  
24 focus on technology as both part of the drivers of  
25 change, as well as a potential place to search for

1 solutions.

2 Today you will of course hear from many of the  
3 constituents that make the Bay Area such a special place.  
4 You'll hear from technologists. You'll hear from  
5 startups. You'll hear from grownup businesses. You'll  
6 hear from scholars and practitioners, and you'll hear  
7 from some researchers.

8 And here at the Berkeley Center for Law and  
9 Technology one of the things that we view as a strength  
10 is the ability to pull together and support activities  
11 such as this that help support a sustained dialogue on  
12 the important issues that are presenting here in  
13 California, in the country and, in fact, the world. And  
14 privacy is, of course, one of them, and one near and dear  
15 to all of our hearts.

16 In thinking about this particular session,  
17 Chris Hoofnagle and I just started leading an advanced  
18 privacy course on the Federal Trade Commission and  
19 Privacy. And I think there is something, it's like a  
20 watershed era for the Federal Trade Commission. You guys  
21 have been at this now for 15 years.

22 And I was fortunate enough to be at the very  
23 first workshop about kind of what were the emerging  
24 consumer issues going to be in this new marketplace. And  
25 Chris and I were talking with our students and they were,

1 like, what were people doing on the Internet in 1995.

2 Nobody was shopping, you know; like what were  
3 they doing; what were the issues? And it's very  
4 interesting to reflect both on what the changes have  
5 been, but also on what some of the constants have been.  
6 And there are a few that I just wanted to tease up.

7 One is, I will never forget then Chairman  
8 Pitofsky talking about the fact that one of the ways in  
9 which Internet was different, the way experiences of  
10 shopping on the Web were different, was that not only did  
11 they know that I chose the steak, but they knew that I  
12 thought about the salmon, right? That was the way he  
13 framed it.

14 And I think we have seen this theme picked up,  
15 perhaps most recently, in some of Commissioner Harbour's  
16 focus on the power of the database of intentions, picking  
17 up on some of John Patel's writing, and the power of all  
18 of these data troves, both the implicit ones that we  
19 leave as we engage in various interactions on the Web,  
20 but also the ones that we are more explicitly choosing to  
21 reveal.

22 The information that we are posting, the  
23 associations that we are revealing, and all of the  
24 information that can be gleaned, the knowledge that can  
25 be created that this is no longer just data, this is

1 fodder for a growing knowledge economy, and how do we  
2 maintain some semblance of a private life, some semblance  
3 of separation as we have these social networks?

4 Are there differences between our private and  
5 our public personas? And how do we think about these  
6 complex issues? I have no doubt that Danny Weitzner at  
7 lunch will give us some particularly sharp examples of  
8 the things that those little data trails can reveal.

9 So I don't want to overstay my welcome up here,  
10 because we have so many interesting people to hear from  
11 today. I wanted to thank all of the people who have made  
12 today possible, both at the Berkeley Center for Law and  
13 Technology, particularly Associate Directors Louise Lee  
14 and David Grady and the Executive Director Robert Barr,  
15 and the Director of Privacy Programs Chris Hoofnagle.

16 I also want to recognize, having spent some  
17 time in D.C. when FTC staff were planning other events  
18 like this, the enormous amount of behind-the-scenes work  
19 that goes on on putting an event like this and getting  
20 the right panels, and the questions. And anybody who's  
21 seen any of the questions they have put together know how  
22 much work and thought has gone into making sure that this  
23 day produces more light than heat.

24 And, finally, I want to give you a little bit  
25 of logistical information. Bathrooms straight back on

1 the left. Question cards in your folders. If you are  
2 participating online, PrivacyRoundtable -- all one word -  
3 - @FTC.gov.

4 And I want to, of course, take just a second to  
5 introduce Commissioner Harbour. She has been, really,  
6 the beacon of independence in many ways on the Federal  
7 Trade Commission on issues of privacy. She's been  
8 staking out and holding ground, bringing in new  
9 perspectives, really speaking clearly in her own voice on  
10 what she thinks the important issues today are.

11 She's been very prescient and forward-looking,  
12 looking to see where the market's going, not just what  
13 the privacy issues are today, but how they are going to  
14 be changing and presenting as we move forward, and I  
15 think incredibly perceptive about the connections between  
16 privacy and antitrust and privacy in a market economy.

17 And for all those reasons I think that we are really  
18 privileged to have her kicking off our meeting today.

19 And I also just want to welcome Director  
20 Vladeck. He has a special place in my heart. When I was  
21 at Georgetown he was the instructor of the public  
22 interest advocacy clinic, advocacy class for the public  
23 interest law scholars. And but for him, I'm certain I  
24 wouldn't be where I am today. So with that, I will now  
25 welcome Commissioner Harbour.

1 (Applause.)

2 COMMISSIONER HARBOUR: Good morning and welcome  
3 to the second FTC Exploring Privacy Roundtable. And I  
4 want to thank Deirdre Mulligan for her kind introductions  
5 and to our hosts here at Berkeley.

6 I would like to briefly offer some opening  
7 thoughts that may frame today's panel discussion. I'll  
8 touch upon social networks, mobile applications, cloud  
9 computing, and the concept of anonymity.

10 To begin, I believe that protecting consumer  
11 privacy is of utmost importance and should be a driving  
12 force for businesses in all stages of product and service  
13 development.

14 Data collection and use can create vast  
15 opportunities for companies, but it also raises a  
16 multitude of privacy issues. And consumers are paying  
17 attention every day. Privacy is emerging as an  
18 increasingly important nonprice dimension of competition.

19 Firms that develop and market pro consumer  
20 privacy tools, embracing what Ontario Privacy  
21 Commissioner Ann Cavoukian calls privacy by design, can  
22 distinguish themselves from their competitors. I could  
23 pick any number of examples to illustrate. For one,  
24 Facebook's recent decision to change default user privacy  
25 settings has been the focus of many media outlets,



1 consumer groups, and users themselves.

2 Previously, the default was that only approved  
3 friends could see profile photos, comments, friends'  
4 lists, and other user data. As a result of recent  
5 Website updates, Facebook users were prompted to update  
6 their privacy settings. The new defaults allowed data to  
7 be shared with all Facebook users, although users were  
8 able to restore more private settings.

9 One significant, potential benefit of  
10 Facebook's actions is that each of its 350 and probably  
11 400 million users by now was confronted with the need to  
12 make decisions about sharing personal data which arguably  
13 empowered users to exercise greater and more deliberate  
14 control over their privacy.

15 On the flip side, however, the new defaults and  
16 other changes meant that consumers had to affirmatively  
17 reinstate their old settings or educate themselves about  
18 the new ones, which they might not have understand. And  
19 that leads to what troubles me about Facebook's actions.

20 The company has offered a number of  
21 explanations for these changes but, based on some senior  
22 executive comments, however, it appears that Facebook was  
23 motivated by a belief that social norms are changing and  
24 that people just don't expect much privacy anymore,  
25 echoing Scott McNeely's famous quip that,

1 just get over it."

2 I think that this attitude demonstrates the  
3 asymmetry between consumer perceptions and business  
4 realities. Consumers do care about their privacy, as  
5 evidenced by recent survey data, and it is also  
6 demonstrated anecdotally by the user outcry following  
7 Facebook's changes to its privacy settings.

8 The problem is consumers often do not  
9 understand how their information is collected and used  
10 online. Facebook's recent experience illustrates the  
11 delicate balance between consumers' desire to share  
12 information, whether for social-networking purposes or  
13 mere convenience, while still maintaining control over  
14 data dissemination and use.

15 Now, we are all here because we know that every  
16 day this balance becomes more difficult to achieve. As  
17 the data set grows larger and richer, not only does the  
18 potential for analysis grow but so does the potential for  
19 profit, a concept that I discussed at the December  
20 Roundtable when I touched on the idea of data as  
21 currency.

22 One of the biggest growth areas is the mobile  
23 space, which is generating incredible amounts of data.  
24 Given the exponential increase in penetration of mobile  
25 devices and services, mobile privacy is crying out for

1 greater attention. Think about it. Worldwide every day  
2 more people use mobile devices than use the Internet.

3 Popular services, both personal and  
4 professional, are migrating to the mobile platform. The  
5 industry-led iPhone Apps Store now offers over 100,000  
6 different applications. And, to date, consumers have  
7 logged over three billion downloads. This is big  
8 business. And now these apps will run on Apple's new  
9 iPad.

10 Unfortunately, though, when it comes to  
11 educating consumers about their privacy implications of  
12 their extensive mobile activity, there is no app for  
13 that. And we cannot and we should not assume that  
14 consumers are shaping their mobile behavior based on a  
15 full understanding of privacy concerns.

16 And to illustrate this point, Danny Widner of  
17 PC Pro Magazine, profiled a very popular iPhone  
18 application called Mobile Allowance that tracks mobile  
19 account details. This application can be an especially  
20 useful tool for people with the pay-as-you-go or  
21 shared-usage plans.

22 When the app is downloaded and installed there  
23 is no mention of privacy. Mr. Widner asked the software  
24 developer whether users had contacted them to ask about  
25 security, and the developer responded that he had

1 received almost no inquiries about the security of the  
2 app or where their details were going.

3 I think that this story is not atypical. In  
4 today's fiercely competitive, mobile app gold rush where  
5 everyone is jockeying for a share of revenues, profits  
6 appear to be paramount to privacy. Consumers may not  
7 know enough to make purchasing decisions based on  
8 comparisons of privacy options.

9 Suppose the average user has 15 third-party  
10 applications, each written by a unique developer with a  
11 different privacy policy or, likely, no policy at all.

12 How likely is it that users truly understand how their  
13 privacy will be affected by what they have downloaded?

14 And given that consumers rarely read typical  
15 privacy disclosures on their big PC screens, should we  
16 really expect that mobile consumers are reading licenses  
17 and privacy policies on tiny smartphone screens? The  
18 proliferation of mobile devices is magnifying existing  
19 concerns about privacy.

20 But given that the mobile ecosystem is still  
21 developing, it may be possible to mitigate these privacy  
22 risks. Here is one suggestion. Apple, for example,  
23 exercises very tight control over third-party developers  
24 of iPhone applications, and it requires all developers to  
25 submit potential new apps for their review.

1           Arguably, Apple could do more to establish a  
2           required baseline level of privacy, or at least privacy  
3           disclosures for approved apps. Similarly, other  
4           devicemakers, along with mobile carriers, could exercise  
5           greater control over the multitudes of third-party  
6           applications. Taking these steps would help minimize the  
7           privacy and security risk to consumers as the market  
8           continues to evolve.

9           And for another twist on the growth of mobile  
10          data, consider the rise of cloud computing. Cloud  
11          applications improve data accessibility and offer other  
12          potential efficiencies, but also raise similar privacy  
13          and security questions.

14          As data leaves the control of individual users  
15          and migrates into the cloud it may be difficult for  
16          consumers to define and articulate their privacy  
17          expectations, let alone make meaningful decisions about  
18          how much data they are willing to share.

19          For example, consumers may not understand that  
20          data sent into the cloud via email, photos, calendars,  
21          and other shared documents may be more easily accessed or  
22          sold to third parties or otherwise used for marketing  
23          purposes.

24          Consumers may not even understand when or how  
25          they are using cloud services, especially with respect to



1 simple computer science techniques enable supposedly  
2 hidden data to be reidentified or deanonymized.

3 Professor Ohm's work mirrors the work of researchers at  
4 the University of Texas at Austin, who have detailed the  
5 use of seemingly anonymous information to uncover the  
6 identity of Twitter users on the Netflix rental service.

7 It also calls to mind what became known as the  
8 AOL incident, where two New York Times journalists  
9 reverse-engineered a user's leaked Internet searches to  
10 establish that person's identity. Now, many pundits had  
11 dismissed that event as unique, but I think it was rather  
12 foreboding.

13 Professor Ohm cautions that we have placed too  
14 much reliance on the purported ability to protect an  
15 individual's identity by deleting or masking critical  
16 pieces of identifying information. If companies cannot  
17 truly deliver and consumers cannot expect anonymization,  
18 then perhaps our faith in current technologies is  
19 misplaced.

20 But let me end on a brighter note. I hope that  
21 as consumers demand more control and protection over  
22 their privacy competition will spur additional innovation  
23 in privacy technology. Chris Hoofnagle, referring to  
24 Google Books, has stated rather artfully, "Privacy by  
25 design requires early intervention."

1           If we are to stay ahead of the technological  
2           curve, we must address the question of privacy by design  
3           sooner rather than later, before it is too late. Thank  
4           you, and I hope you enjoy today's Privacy Roundtable.

5           (Applause.)

6           DIRECTOR OLSEN: Thank you, Commissioner  
7           Harbour.

8           We now have David Vladeck joining us. He's the  
9           Director of the Bureau of Consumer Protection. Privacy,  
10          as I think all of you know, has been a major focus of his  
11          since he joined the Commission, and we are pleased to  
12          have him offer opening remarks.

13          (Applause.)

14          DIRECTOR VLADECK: Thanks. Though my staff has  
15          put me behind Commissioner Harbour and Professor  
16          Mulligan, two very tough acts to follow, I'll try to keep  
17          up the pace. It's great to be here in California. John  
18          Kennedy once remarked that D.C., Washington, D.C., is a  
19          city of southern efficiency and northern charm.

20          Berkeley is a city of enormous charm and,  
21          fortunately, we decided we would come to where the  
22          technologists were. We have come to the mountain in  
23          Berkeley to tap into the technological community that  
24          makes its home here. And we really value learning today  
25          from people who work on a day-to-day basis at the



1 intersection of technology and privacy.

2 But before I begin I want to say thanks to a  
3 number of people who have made today's event happen. Of  
4 course, my former student and colleague, Deirdre  
5 Mulligan; Chris Hoofnagle. We have always rued Chris'  
6 departure from the East Coast to the West; David Grady,  
7 Louise Lee, and the Berkeley Center for Law and  
8 Technology for cohosting this event with us.

9 I'd like to thank Dean Edley and the law school  
10 here at Boalt Hall for providing this lovely venue. I  
11 want to thank our colleague, Danny Weitzner, from the  
12 Commerce Department for coming out here. We have been  
13 working with the Commerce Department, we have been  
14 working with Danny, and we look forward to continuing our  
15 partnership as we move forward.

16 And finally and most importantly, I'd like to  
17 thank our incredibly accomplished groups of panelists.  
18 You are why we are here. We are grateful for your  
19 expertise, and we look forward to hearing from you today.  
20 I want to start with you by talking a little about our  
21 December roundtable.

22 Today's roundtable will build on some of the  
23 lessons that we learned. And I think there are three key  
24 ones.

25 First, that consumers have little understanding

1 of commercial information collecting practices. They  
2 don't really understand what data is collected about  
3 them, how that data is used and shared, and whether and  
4 how they can exercise control over their data.

5 For example, we heard that consumers are  
6 largely unaware of the practices in the data brokering  
7 industry, particularly the extent and nature of personal  
8 information that is regularly collected and sold. In the  
9 online world we heard that the practice of behavioral  
advertising may not be clear to consumers.



1 their own privacy.

2 Now today's roundtable is organized around  
3 themes of technology and privacy -- no surprise we are at  
4 Berkeley -- and we want to build on what we learned in  
5 December. I've always said that as policymakers we  
6 should encourage innovation and technology for the  
7 benefit of consumers.

8 And I think Microsoft's CEO Steve Ballmer  
9 summed this up about as well as it could be summed up.  
10 He said: It empowers people to do what they want to do.  
11 It lets people be creative. It lets people be  
12 productive. It lets people learn things they didn't  
13 think they could learn before, and so in a sense it's all  
14 about potential. But as we know, potential is a two-way  
15 street and technology raises public policy challenges, as  
16 well.

17 But to quote from another public figure, author  
18 Alice Kahn, she's aptly stated, and I'm quoting, "For a  
19 list of all the ways that technologies have failed to  
20 improve the quality of life, please press three."

21 The point is that, of course, technology  
22 improves our lives, but in the context of today's  
23 discussion it can enhance our privacy, as well.

24 But it raises some challenges, and we are going  
25 to talk about those today. Indeed, our opening panel



1 others can scrutinize the minutia of our lives, future  
2 employers, current bosses or, even worse for my kids,  
3 their parents might try to friend them.

4 So as the amount of personal information shared  
5 through these services grows and, as Commissioner Harbour  
6 pointed out, as the number of third-party applications  
7 with access to such information grows, it's important  
8 that consumers understand and know how their data is  
9 being shared.

10 Our expert panels will focus on these issues  
11 and explore the extent to which transparency and  
12 meaningful control exist for consumers when they use  
13 these devices. Similarly, cloud computing offers  
14 significant consumer benefit, no doubt about it. Storage  
15 in the cloud may be cheaper and may reduce the need for  
16 businesses and consumers to purchase, operate, and  
17 maintain software and hardware themselves.

18 At the same time, storing data on remote  
19 computers raises serious privacy and security concerns.  
20 For example, the ability of cloud computing services to  
21 collect -- excuse me -- to collect and centrally store  
22 increasing amounts of consumer data, combined with the  
4e when they use

1 by consumers. Our panelists are sure to shine some  
2 sunlight on this practice of cloud computing.

3 Third, increasingly, ubiquitous mobile devices  
4 have brought tremendous benefits to consumers. They are  
5 so versatile that some people forget that you can  
6 actually use them to make phone calls, but we need to  
7 examine the privacy considerations here, as well.

8 For example, how is location-based information  
9 collected, shared, and used? What constraints are being  
10 placed on that practice? How do companies obtain  
11 informed consent for such practices on a PDA with a  
12 screen this size? Anyone going to read a disclosure  
13 policy on something like this? Our panelists will help  
14 us analyze these issues in detail.

15 Our last panel will highlight ways in which  
16 companies are building privacy into their products and

1 represent the sum total of our work in privacy.

2 We intend to maintain an active law enforcement  
3 presence to protect consumers from unfair and deceptive  
4 privacy practices. As but one example, we are currently  
5 examining practices that undermine the tools consumers  
6 can use to opt out of behavioral advertising, and we hope  
7 to announce law enforcement actions in this area this  
8 year.

9 With that, it's time to let our expert  
10 panelists take the floor. Thank you very much for  
11 coming. We very much look forward to hearing from you  
12 all today. Thank you.

13 (Applause.)

14 DIRECTOR OLSEN: I'd like to ask the first  
15 panel of panelists to come up to the stage. We will have  
16 a couple of minutes while we get settled, if anyone wants  
17 to take a short break or grab a cup of coffee. And we'll  
18 start promptly at 9:15. Thank you.

19 (Recess taken from 9:06 a.m. to 9:14 a.m.)

20

21

22

23

24

25



1 PANEL 1: TECHNOLOGY AND PRIVACY

2 MS. HARRINGTON-McBRIDE: Good morning,  
3 everyone. Welcome to our first panel of Roundtable Two,  
4 entitled Technology and Privacy, where perhaps, not  
5 surprisingly, given the title of the panel, we will  
6 examine the tensions between technology and privacy.

7 Technology, as we all know, provides enormous  
8 benefits to our daily lives, and our lives have all been  
9 changed significantly in the ways that our other speakers  
10 this morning have discussed.

11 I don't know that I can begin to approximate  
12 Steve Ballmer's eloquence on the topic, but there is no  
13 question that we are now all staying connected and  
14 learning in different ways than we did even five or ten  
15 years ago, and that there are ways that our productivity  
16 has increased and that our lives, again, have been  
17 changed immeasurably, personally and professionally.

18 So the benefits to technology I think are  
19 unquestioned. It's also, I think, unquestioned that  
20 there are times when technologies may impinge on  
21 individuals' privacy. And so that's what we are planning  
22 to do today, is to talk about this natural tension that  
23 has developed.

24 In the escalation of technologies to be used in  
25 ways to improve our lives we have begun to see that there

1 are ways in which they may also detract from our privacy.

2 So in this panel we are going to highlight the  
3 arms race that David Vladeck mentioned, as new and  
4 repurposed technologies are used to collect ever more  
5 data about our habits, our behaviors and interests.

6 In some cases this technology can be used to  
7 facilitate data collection in ways that are opaque to  
8 consumers. And in some instances the collection itself,  
9 the methods that are used, may override consumers' stated  
10 preferences. We are going to talk today about some uses  
11 of technology, specifically that meet both of these  
12 criteria.

13 That is, they are opaque and they override  
14 consumers' stated preferences. A couple of examples of  
15 those are Flash cookies, which now have been used to  
16 subvert consumers' preferences regarding cookie-tracking  
17 and also offline surveillance technologies.

18 We are also going to take a close look at  
19 another topic that was mentioned in Commissioner  
20 Harbour's opening remarks. And that is reidentification  
21 of data.

22 We are going to look at advances in technology  
23 that challenge our assumption about how anonymity works  
24 and what it means in a technology-driven world where it  
25 may be possible to amalgamate individual bits of data and

1 recombine them in ways that lead to identification of  
2 people who previously thought they could not be known.

3 In the second half of the panel we are going to  
4 talk about the ways that technology can actually assist  
5 in providing individual consumers their privacy. We will  
6 look at ways that technology can be used to facilitate  
7 this. As David mentioned, it has been used already in  
8 some creative ways in providing new opt-out opportunities  
9 for consumers.

10 Certainly, there are interesting developments  
11 in the mobile space regarding new notices that do have to  
12 take advantage of the fact that they are being given on  
13 two-and-a-half-inch screens. And so our goal today is to  
14 look as holistically as we can about how technology can  
15 work in consumers' favor, how we can leverage the  
16 technologies that have been developed to provide benefit  
17 to consumers, and to examine some of the uses that may

1 it's the only fair way to do things, by these eight

2 excellent panelists. We have with us:

3 Pam Dixon, who is the Executive Director of the  
4 World Privacy Forum, immediately to my left; to Pam's  
5 left,

6 Peter Eckersley, a Staff Technologist with the  
7 Electronic Frontier Foundation; to Peter's left,

8 Eric Goldman, Associate Professor at Santa  
9 Clara University School of Law; to Eric's left,

10 Chris Jay Hoofnagle, a lecturer here at the  
11 University of California, Berkeley School of Law; to  
12 Chris' left,

13 Arvind Narayanan, a Postdoctoral Fellow at  
14 Stanford University; to Arvind's left,

15 Sid Stamm, and Sid is a new name for you. If  
16 you are looking at your packet of information and looking  
17 at the agenda, Sid has very graciously agreed to step up  
18 and fill in for a colleague of his, Mike Shaver, at  
19 Mozilla, who has taken ill and is unable to be with us.

20 Mike, if you are watching on the Webcast, we  
21 are wishing you well and hoping that you can be with us  
22 another time.

23 Sid, we are extremely grateful that you were  
24 able to step in. Sid is a self-described privacy and  
25 security nut. To Sid's left we have:

Scott Taylor, who is the Chief Privacy Officer

1 need to cut things short. So just let us know if you  
2 have an interest in speaking, and we will certainly try  
3 to get to you.

4 Also I wanted to say that we encourage  
5 questions from the audience. From our audience here at  
6 Booth Auditorium, if you have questions there are  
7 question cards inside the packets that you were given  
8 when you checked in today. Feel free to jot your  
9 questions down. And throughout this morning's session we  
10 will have volunteers going through the aisles and  
11 collecting them. You'll just need to pass them down to  
12 the aisle.

13 We will do this at a couple of points this  
14 morning. If you have a question card ready and you want  
15 to hold it up, that's fine. But at about 45 minutes in  
16 we will do a collection and get those questions and try  
17 to ask some of them here on the panel. We will also do  
18 one a few minutes from the end of the panel.

19 If you are in the Webcast audience you, too,  
20 are welcome to participate by submitting questions to the  
21 address given at the very beginning. And that is,  
22 PrivacyRoundtable -- all one word -- @FTC.gov. We will  
23 be monitoring that account and escalating those questions  
24 up here, as well.

25 So we would be delighted to hear from you. We



1 probably by accident, it turns out that these cookies,  
2 although they function as a tracking mechanism, they  
3 don't respect the controls that users are given to turn  
4 off, limit, or block ordinary cookies.

5 So people who think that they have configured  
6 their browser to block cookies and not be tracked by  
7 them, if you go and look at their computers, if they have  
8 the Flash Player installed they will actually be tracked  
9 by a large number of these Flash cookies.

10 So there is a case where technology clearly  
11 circumvents, by accident or by design, the intentions  
12 that the user clearly had to not be tracked.

13 MS. HARRINGTON-McBRIDE: Thank you.

14 Chris, do you have anything to add on that  
15 about consumers' expectations? For example, if a  
16 consumer is diligent, knows the ropes enough on their  
17 computer to know that they ought to delete their cookies,  
18 what effect -- there'll be no effect, presumptively, on  
19 Flash cookies, if they are going into to just  
20 traditionally clear their cookies. So --

21 PROFESSOR HOOFNAGLE: Yes. As Peter mentioned,  
22 the Flash cookies are not controlled by the browser  
23 settings. And this was an advantage, according to some  
24 advertising companies. In fact, there is a press  
25 release from one advertising company that simply says



1 consumers don't know about this avenue, and we can track  
2 people even if they delete their cookies.

3 So there is a clear kind of intent to evade  
4 consumer control. And it's one example of a clear  
5 opportunity for the Federal Trade Commission to remedy a  
6 problem.

7 (Laughter.)

8 MS. HARRINGTON-McBRIDE: Well, I'd like to  
9 continue with the panel, but I have some work to do back  
10 at the office. Does anyone else on the panel have any  
11 thoughts about this general topic? Arvind?

12 DR. NARAYANAN: I want to bring up the point  
13 that maybe one reason that Flash, in particular, has sort  
14 of come into this role as a supercookie might be because  
15 it's a proprietary standard. This has some effects in  
16 terms of transparency. It's much harder to create an  
17 open-source implementation, for example, because it gives  
18 browsers, as well as users, less control over what  
19 happens inside of Flash.

20 The importance of not having proprietary  
21 standards for the Web has recently been a topic of  
22 discussion, and perhaps among all the disadvantages of  
23 proprietary standards or de facto proprietary standards,  
24 I should say, one should add that it's bad for privacy,  
25 as well.

1 MS. HARRINGTON-McBRIDE: All right. Sid?

2 MR. STAMM: I'd also like to add that Flash  
3 wasn't originally purposed for this, because well, not  
4 everybody had Flash installed, but now it's so ubiquitous  
5 on the Web it can be considered about as effective as  
6 regular cookies.

7 MS. HARRINGTON-McBRIDE: Pam.

8 MS. DIXON: Another thing to consider is the  
9 consumers' perspective on this issue. In order to remove  
10 Flash cookies you have to use the controls proposed by  
11 the company, and they are very challenging to use. And I  
12 think that most consumers find them enormously  
13 frustrating. And this also points up an area of tension:  
14 What do you do about making a remediation when you might  
15 have 20 proprietary technologies? Do consumers need to  
16 go to 20 different controls from 20 different companies?  
17 This is an issue.

18 MS. HARRINGTON-McBRIDE: You all bring up a  
19 good point. It was just in the news, this week I  
20 believe, that Adobe has just released a new version of  
21 Flash 10.1 or is on the verge of so doing. And it's  
22 reported to automatically recognize that the private  
23 browsing mode currently found in several of the Internet  
24 browsers, they recognize this mode and they abide by its  
25 rules, clearing data that's created in a session.



1 browser when the user wants to enter a private browsing  
2 mode we had to create some sort of signal the browser  
3 could send to Adobe Flash to let it know, hey, the user  
4 wants to be in private mode.

5 So 10.1 is an example of a successful signal  
6 being established between the browser and Adobe Flash.  
7 And we are working on more signals that we can send Adobe  
8 Flash so that they can listen to things like, I want to  
9 clear all my cookies, or all my history.

10 MS. HARRINGTON-McBRIDE: Anne?

11 MS. TOTH: I think it's also important to  
12 understand the scope of this problem. I think there is  
13 definitely a potential privacy issue there. And there  
14 are some companies who are using Flash cookies in this  
15 way, but if you look across the industry and you look at  
16 the largest ad network players and the folks who are  
17 abiding by self-regulatory standards, you know, it's not  
18 that common among the major ad network players.

19 And companies like ours, like at Yahoo!, we  
20 disclose what we do with Flash cookies. We explain where  
21 you can actually modify them or delete them if you like,  
22 but we are not -- when we offer choices to consumers, we  
23 are not trying to -- we would never circumvent that  
24 choice by trying to slip one by in a Flash cookie.

25 so I think if you look at the role of self-

1 regulation here, companies are basically raising their  
2 hand and saying, we will not do this. And it's just  
3 another point of differentiation.

4 So I just want to make sure that we recognize  
5 that it's not ubiquitous, that most companies are not  
6 using Flash cookies to do online behavioral advertising  
7 in this way. And a lot of companies have already said:  
8 We won't do that.

9 MS. HARRINGTON-McBRIDE: Okay.

10 PROFESSOR HOOFNAGLE: A minor point.

11 MS. HARRINGTON-McBRIDE: Um-hum.

12 PROFESSOR HOOFNAGLE: I think it shows an  
13 important difference between first-party companies that  
14 consumers have a relationship with, like Yahoo! and HP,  
15 who do a lot to establish trust, and then these third  
16 parties that don't have any real consumer relationship.  
17 And from a statutory framework they look more like  
18 consumer-reporting agencies than a situation where a  
19 consumer has a direct relationship where market forces  
20 can be brought to bear on their conduct.

21 So I think this is another area where the FTC  
22 has opportunities to try to address the gaps between  
23 first and third-party entities. And I know Eric has  
24 something to say about that.

25 (Laughter.)

1 MS. HARRINGTON-McBRIDE: Eric, please weigh in.

2 PROFESSOR GOLDMAN: I think the discussion

3 about Flash cookies is really just a microcosm of that

4 introductory remark about a technological arms races.

And so, as usual, we have to ask the querout T(c-404 -2.2732c07l.2404 0 TD (4 )Tj 252404 -2.2678 TD (

1 developing newer technologies to find new ways to collect  
2 data. And, again, some of these are nonopaque. Some of  
3 these are perhaps in circumvention of consumers' wishes.

4 There has been a lot of discussion about other  
5 supercookies -- this is just one of that genre -- and  
6 other methods of tracking that may be more sophisticated  
7 and less well known.

8 Peter, I know you have done some work on this.  
9 Could you tell us a little bit about it?

10 MR. ECKERSLEY: Well, I wouldn't say that the  
11 other kinds of supercookies are more sophisticated than  
12 Flash cookies. I think all cookies, fundamentally from a  
13 computer science point of view, they are very simple  
14 technologies. They're just data storage. But the  
15 problem is that there are about five or six of these  
16 other kinds of supercookies.

17 In addition to Flash cookies, there are  
18 dumb-storage objects. There are HTML 5 databases. There  
19 are Silverlight cookies, Microsoft Silverlight cookies.  
20 There are Google Gears cookies. And I have to give some  
21 props to Google for having -- they tend to pop up a  
22 little notice before you get supercookied by Google  
23 Gears. So maybe that technology is a little less  
24 dangerous than some of the other supercookies.

25 But what we have got is the -- and Microsoft

1 Internet Explorer also has a thing called user data. So  
2 there are all these different things. And if you want to  
3 not be tracked by cookie-like mechanisms, you need to not  
4 only block cookies but -- and Flash cookies, you need to  
5 go in and modify settings potentially for a lot of these.

6 Now, some of them, some of them do better jobs  
at respecting user preferences. I know that Mozilla better jobs



1 you will actually not be able to take advantage of some  
2 of the value that cookies provide to you and that exists,  
3 you know, in the Internet space, but offline, as well.

4         Years ago, I remember I went to an  
5 accessibility conference, actually, so the topic was all  
6 about assistive technology. And I heard Vint Cerf speak.  
7 And it wasn't a privacy event. But he was talking about  
8 the wonders of the day when you could actually -- when  
9 your pantry could order groceries for you on the Internet  
10 because everything is RFID-tagged and your pantry would  
11 tell the Internet that you were down on milk and cereal  
12 and it would automatically order it for you, and wouldn't  
13 that be an amazing world.

14         And as a person with three small children, a  
15 busy life, and all of this going on I just thought, you  
16 know, wouldn't it be great if I could walk into a grocery  
17 store, put everything in my cart, walk straight out of  
18 the grocery store, not have to go through the checkout  
19 line and stand there and think, do I have 15 items or 20  
20 items; got to be here or there.

21         I can just walk out. I can charge my card  
22 because everything is labeled, and it would just be  
23 superconvenient. And then I go home, and it's all great.  
24 It can even reorder for me. But there are obviously  
25 privacy challenges as to that kind of a world.

1           Whereas, I might want to be able to reorder  
2           milk without having to think about it, I certainly  
3           wouldn't want someone walking by my house saying, you  
4           know, Anne, you only have three Tampax left. You know,  
5           that's not something that I would want. So there has got  
6           to be a protection in place to make sure that, you know,  
7           you are able to control harm and add protective layers  
8           without actually taking away the consumer benefit that  
9           technology can bring us.

10           MS. HARRINGTON-McBRIDE: Scott.

11           MR. TAYLOR: Yes. I think Anne really brings  
12           up a good point, and everybody on the panel's been  
13           talking about it, that every technology that brings  
14           benefits, because we can talk about cookies and we can  
15           talk about all the benefits that come from the fact that  
16           you can go back to a site and it remembers your user ID,  
17           the customization that comes from it can very much be  
18           used in nefarious ways.

19           And I think that every technology that we are  
20           going to talk about that brings benefit or that maybe was  
21           created to create value, whether it be to the company, or  
22           organization, or to the consumer themselves, can be often  
23           turned around and used in bad ways.

24           And I think what's being highlighted just in  
25           this first discussion is the fact that technology itself

1 isn't necessarily bad, but we have got to ensure, as Anne  
2 was highlighting with Yahoo!, that organizations are held  
3 accountable to understand the risks that these  
4 technologies pose, as well as the benefits, and that they  
5 are held accountable to the obligations and the promises  
6 that they make, whether those are driven by regulation or  
7 their own self-assertions.

8           But the administrative controls that sit  
9 between either regulation or expectations and the  
10 technologies that can help us deliver both value, as well  
11 as privacy protections, those administrative controls and  
12 the accountability of organizations becomes critical,  
13 because I often -- we were talking in our prep for -- for  
14 the panel about RFID, and then new technologies being  
15 created to scramble RFID so that people can't read it if  
16 it's something that you are walking past an RFID reader.

17           So we are putting technology on top of  
18 technology to try to solve problems, when, in fact, we  
19 need to focus on the fact that the organizations using  
20 these technologies need to be accountable for how they  
21 are using them, and the risks, and the values, the  
22 benefits that come from that.

23           So I think that that concept of accountability  
24 and administrative controls really is going to be some  
25 place we need to focus on if we are ever going to try to

1 solve the problem of the good and the bad, the double-  
2 edge sword that Commissioner Harbour talked about.

3 MS. HARRINGTON-McBRIDE: I think that's an  
4 excellent point. Before we get to that discussion,  
5 though, which we absolutely will do toward the end of  
6 this entire session, let me ask a little bit about  
7 something that Anne has alluded to, which is the offline  
8 use of tracking. So tracking, whether through RFID or  
9 the information that our electrical systems may now put  
10 out to the smart grid; tracking that happens in offline

10 aad c h e n a m p h a w h i t e F: 2 4 0 2 r h d j ) 2 j 2 4 8 1 5 a 9 2 2 2 4 4 3 0 4 C o s i e n t e r t o 4 0 6 3 a b z e d v a d s 4 8 e t o w a r d t r a

1 the screens at Whole Foods in Chicago exactly know that  
2 this is going on. I looked at the privacy policies in  
3 Whole Foods. No disclosure of this. Not that someone  
4 would be cruising around looking at produce thinking  
5 about a Website privacy policy in the first place. So  
6 this raises a lot of issues.

7 When we started to look at this issue and do  
8 some research on it we found an industry document called  
9 best practices, recommended code of conduct for consumer  
10 tracking methods. And it's a self-regulatory document.  
11 And they basically said technological advances have made  
12 it enormously simple to track consumers' every move in  
13 public and private spaces and keep it for longevity,  
14 using security camera footage and new footage obtained by  
15 the digital signage network.

16 So what does this mean for consumers? The big  
17 problem here is that your face, your body, your gender,

1 image is matched with their name or home address, it's  
2 not personally identifiable. So this is putting enormous  
3 tension on an old conflict which is, if a person is  
4 walking in public or in a private space, but they are  
5 essentially in public, they have no privacy rights.  
6 You've given them up by being in public.

7 But in an era of essentially unrestrained, you  
8 know, recordings and imagetaking, I think new tensions  
9 are being put on that. And what Anne describes as, you  
10 know, the RFID tracking, it already exists in stores.  
11 It's called path tracking, and there is actually products  
12 available for it. We have illustrations in our report.

13 But the thing is, is that do we want to have  
14 principles that control that, and I think the answer is  
15 yes. And I think it's a very significant opportunity for  
16 the FTC here to come up with principles that control  
17 broad privacy issues in regards to disclosure of tracking  
18 of consumers, whether they are in public or in private.  
19 I think we need to look at that afresh and anew.

20 MS. HARRINGTON-McBRIDE: Deirdre Mulligan  
21 mentioned at the very beginning of our session today that  
22 Chairman Pitofsky, who apparently was, in this regard,  
23 extraordinarily prescient, noted that you may choose the  
24 steak, but they will know that you thought about the  
25 salmon.

1           Apparently, you don't need to shop online for  
2           that to be the case, according to this new information.

3           This is an emerging field. Does anyone else on the panel  
4           --

5           I see, Arvind, you have your tag up. Do you  
6           know anything about the prevalence of this? Do you have  
7           thoughts about what to do in a ubiquitous data collection  
8           environment? What solutions can you put into play?

9           DR. NARAYANAN: That's a great question. I  
10          want to make a slightly related point, which is that in  
11          addition to tracking increasing in the offline world, the  
12          difference between online and offline tracking is  
13          increasingly becoming thinner and even vanishing.

14          My favorite example of this is the fact that  
15          information about who you are friends with on online  
16          social networks, as well as what kind of comments you  
17          make, get aggregated, both across users and across social  
18          networks by companies such as Rapleaf. And then this  
19          gets fed into, you know, credit organizations, and then  
20          banks use this to make lending decisions about you.

21          And so the problem is not only that there is  
22          this separate kind of tracking going on, but also that  
23          it's all coming together.

24          MS. HARRINGTON-McBRIDE: Anne.

25          MS. TOTH: I think that as we think about these

- 1 things, restrictions on use rather than perhaps even
- 2 collection might be more useful. So if I'm at Whole





1 use technology to empower consumers to say: This is how  
2 you know what we know and this is how you control what we  
3 can use about you.

4 I haven't found an offline tool that allows me  
5 to see how a company has segmented me or given me access  
6 to that degree of information or degree of control. So  
7 I'm sure that I will be aggressively shot down by  
8 somebody on the panel. But if I say that, you know, I  
9 think there might actually almost be more privacy in some  
10 respects online than there exists in the offline world,  
11 or at least that we have been incented to give those  
12 controls to consumers more and more.

13 I think actually just yesterday another ad  
14 network opened the kimono on, you know, profiles that  
15 they are giving users access to and control over. So  
16 reactions?

17 MS. HARRINGTON-McBRIDE: I'm sure there are. I  
18 see, I think, more tents standing than laying down now.  
19 Scott.

20 MR. TAYLOR: I just wanted to comment on this  
21 concept of use versus collection. I think that there is  
22 a lot of merit to that. Collection continues to be  
23 important and I think, more important than anything, the  
24 transparency that comes at the point of collection.

25 But I do believe that use more and more is

1 becoming the lens that we need to think about. And I  
2 believe that that's true, because that's ultimately where  
3 the risk and the harm, a big part of it, will come from,  
4 is how that information is used. I think it's much  
5 easier for us in good transparency to explain how that  
6 information will be used, not only, as Chris was saying,  
7 in a first-party sense, but how that use might follow  
8 into a third-party sense.

9 Chris asked the question of how could  
10 technology help to solve that. I truly believe that a  
11 lot of the work that is being done around the concept of  
12 sticky data is very important that tags around  
13 obligations and consent that was given or collected,  
14 obtained, for the data, that it follows the data through  
15 its lifetime in an appropriate fashion.

16 It's a complex thing, but we have many examples  
17 of where that type of technology's being used today in  
18 network advertising for revenue, as an example.

19 MS. HARRINGTON-McBRIDE: And that's actually --  
20 you know -- I hate to cut you off, Scott, but I do -- we  
21 are actually going to devote a fair amount of time to  
22 that right at the end of the panel. And I want to get  
23 back to all those things that businesses can do.

24 But to air a little bit more about the specific  
25 issue of tracking, I mean, Anne raises the point that,

1       you know, this is not maybe secret data anyway. Shopper  
2       loyalty cards and other mechanisms perhaps allow for some  
3       transparency already.

4               How would the introduction of facial  
5       recognition, heat mapping in stores, tracking and  
6       surveillance technologies deployed in retail stores  
7       beyond what we already know to be fairly commonly used,  
8       how would that impact the privacy landscape?

9               Arvind, is that a point that you would care to  
10       speak to?

11              DR. NARAYANAN: I was going to make a point  
      about?

1 your name being the big idea online, it's going to be  
2 your image.

3 So a captured image of a person, if you can  
4 identify that person by their name, that's going to be  
5 like gold for commercial data brokers in the coming  
6 years. And we have got to think about that collection  
7 and that kind of tagging. And I do think we have to  
8 focus on the collection of data, especially when it's  
9 surreptitious.

10 I just don't think it's proper to have a data  
11 collection mechanism that consumers do not know about.  
12 That defies their expectation of privacy.

13 MS. HARRINGTON-McBRIDE: All right. With that,  
14 Peter, I'm going to give you the last word for this  
15 segment.

16 MR. ECKERSLEY: Excellent. Thank you.

17 So something that Anne said before I think  
18 raised an important point, which is the fair information  
19 practice of access. Now, I think a lot of us on the  
20 privacy advocacy side think that the situation right now  
21 is so broken that the fair information practices won't  
22 save us.

23 Even if we could actually implement them all,  
24 there are other kinds of regulation or help that we  
25 probably need in order to get consumers some privacy

1 back. But having said that, the fair information  
2 practice of access is a really interesting one and one  
3 that I think, if we could do some more work in developing  
4 it and implementing it in a sensible way, might be a  
5 powerful light to shine into the kind of dark void of  
6 data collection.

7 Now, what would that look like? I think one  
8 thing it would have to look like is not you having to go  
9 to dozens of different data brokers, in-store loyalty  
10 cards, and Yahoo!, and lots of other people and ask them  
11 all through different interfaces what data they have  
12 about you.

13 It would have to be a single place that you  
14 could go where these companies were required to report  
15 that they have collected data about you and tell you what  
16 it is, and let you go in and delete it and say: Go away  
127 and never collect data about me agognb

IAa si02.841lectintr oA -2w.5 nerequir2.8415 -2.2678 TD (4D (10 )Tj 2.8415 -1/o nbeoplr23away 0 C

1 terms of giving consumers more control.

2 MS. HARRINGTON-McBRIDE: Well, I think we have  
3 almost 45 more minutes on the panel. So let's try to  
4 work on that. Lori.

5 MS. GARRISON: Well, thank you.

6 I believe that we have already begun to touch  
7 on the problem of the merging of the data, the  
8 multiplicity of individual handheld devices and the  
9 problems that arise now with de-anonymization.

10 So I want to turn to that issue here and ask  
11 Arvind, to start off, has technology made anonymity  
12 difficult, if not impossible, to achieve?

13 DR. NARAYANAN: That's a great question. And  
14 when I think of anonymity, from at least a computer  
15 science perspective, I tend to divide it into these two  
16 very different categories. One is what we call  
17 communications anonymity and the other is data anonymity.

18 Communications anonymity would go to questions  
19 of something like what's Toro enables, the anonymity  
20 network. Can there be a group of people who are  
21 communicating with each other so that anybody who's  
22 snooping, let's say a government interested in  
23 surveillance or, really, anybody else, is not able to  
24 tell who's communicating with whom?

25 And in that sense technology has, I think, made

1 things a lot better to where it's been very helpful to,  
2 you know, lots of peoples around the world.

3 The other question, though, is data anonymity.  
4 And there I think the story has been almost entirely  
5 negative. The sort of default solution for entering data  
6 anonymity up until now has been deidentification, and the  
7 track record there has not been very good at all. We  
8 have had the AOL search data incident. There is the  
9 de-anonymization of Netflix and other social-networking  
10 data sets. And these incidents just keep happening.

11 And so the lesson really here is that when you  
12 are looking at data that's as rich as is being collected  
13 now, and the term that we use as far as their  
14 high-dimensional data, which means that you have data  
15 about individual consumers and there is a lot of points  
16 of information going back to their activities over, say,  
17 years, or something like that. And here it's not clear  
18 that there is anything that technology can do to ensure  
19 data anonymization.

20 So if I could summarize that I would say  
21 communications anonymity has become a lot easier, but the  
22 more relevant thing to this panel is data anonymization.  
23 And that's not been a happy story so far.

24 MS. GARRISON: Chris, do you have a comment?

25 PROFESSOR HOOFNAGLE: Yes. And this relates





1 focused on this distinction between what is  
2 personally-identifiable information and that's what's to  
3 be protected and secured, and then nonpersonal  
4 identifiable information where you don't have as great a  
5 concern because it doesn't link to an individual.

6 Given where we are with the technology now,  
7 does this distinction make any sense anymore? I'm going  
8 to throw it open. Does anyone have comment or question  
9 or a point on this, or...? Scott, would you like to  
10 begin?

11 MR. TAYLOR: You know, I think that PII in its  
12 traditional sense, 25 years ago when I was doing direct  
13 marketing it made a lot of sense, but I think it's  
14 becoming less and less useful. And I think that's been  
15 illustrated just this morning that, you know, we are only  
16 one piece of data away from identifying people or  
17 reidentifying deanonymized data.

18 And I really think that PII has had a place,  
19 but we need to think about data in a different way. I'm  
20 not saying that all data is impactful, but a lot of data  
21 is impactful. And I really think that it behooves us to  
22 start thinking about the next generation of what PII was  
23 and think about how we can oversee and protect impactful  
24 information.

25 Some data never will have any real impact.

1 Anne's brought up some examples of where things are  
2 pretty innocuous. But the ability in this networked  
3 environment to combine and combine and combine data, at  
4 some point impact can be achieved. And that impact can  
5 come with it value and benefits, but it can also be  
6 harmful. And I think that we need to think about that in  
7 a very different way going forward.

8 MS. GARRISON: Scott, on that point, is there a  
9 way in which you draw some sort of a boundary or a  
10 distinction that's workable as you move forward? In  
11 other words, what we have been doing is, you say name,  
12 address, you know, contact information, so forth, that's  
13 specifically, personally identifiable.

14 But there are other kinds of information where  
15 it was just, you know, just the fact that you have an  
16 account somewhere, but not information about the account,  
17 or that you live in a certain city without anything more  
18 specific? I mean, does it make sense to have those  
19 specific kinds of categories, or do we need to look at it  
20 differently? I'm trying to figure out what you mean by  
21 "impactful."

22 MR. TAYLOR: Yes. I think that it's a good  
23 example, and it's a good question. The example of being  
24 able to identify somebody and to create some impact is  
25 really what I'm talking about. So data can be combined,

1 and that data suddenly becomes personally identifiable.  
2 The data by itself in different sources may not be. And  
3 we have talked a lot about IP addresses.

4 But we can all think of examples where an IP  
5 address could be considered in isolation nonPII. But we  
6 can also think of lots of examples where that can be  
7 combined with other information to quickly become PII or  
8 something that's personally identifiable.

9 I think that we could create those boundaries.  
10 I don't necessarily have them in my mind at this moment,  
11 but I think that the point is we need to think about it  
12 in a very different way. I don't think that PII by  
13 itself solves the problem, because of the nature of how  
14 data can be combined, and the ubiquitous collection that  
15 we were talking about earlier.

16 MS. GARRISON: Okay. Lots of cards out. Sid.

17 MR. STAMM: Yes. I want to agree with Scott.

18 Every bit of information you can get about  
19 somebody is going to tell you a little bit of something  
20 about them. And this constellation of information that  
21 you can collect online and offline about people is  
22 exactly what Peter was talking about before.

23 Each bit of data may not be interesting in  
24 itself, but it has some sort of significance towards the  
25 person's identity, the person who owns the data. And

1 with enough of these little bits of data you can end up  
2 with something that's personally identifiable.

3 MS. GARRISON: And also the particular piece of  
4 data itself may have once been nonidentifiable, but now  
5 they become identifiable. So, for example, an IP  
6 address, as we move into IPB6 and individuals get static  
7 IP addresses, we are going to have a reverse lookup, it's  
8 not that far away, where it will be tied not just to a  
9 device, but that particular device to one single  
10 individual.

11 Arvind.

12 DR. NARAYANAN: Yes. In general, I agree with  
13 Scott and Sid. And my sense is that PII is not a helpful  
14 concept going forward in the context of data privacy.  
15 Let me offer a comment about categories of PII that you  
16 brought up. I think an interesting thing that happened  
17 is that there are two different contexts in which PII is  
18 used in privacy law.

19 One is in breach notification laws, which a  
number

1        need to be notified.

2                There are also privacy laws, which are about a  
3        completely different issue. It's not about financial  
4        information. It's about all information in general. In  
5        these laws they also use the term "PII," but in a very  
5

1 independent of each other, can be added up. And the  
2 mathematics is if you hit 33 independent bits of  
3 information about a person's identity that's enough to  
4 make them globally unique on this planet with seven  
5 billion people.

6 Now, how does this work in practice?  
7 Conveniently, we actually -- I don't want to talk -- brag  
8 about EFF projects too much today, but we launched a  
9 project yesterday which does an example of this for Web  
10 browsers.

11 So if you go to the EFF.org Website and then  
12 click through to this thing called Panopticlick, you can  
13 see this theory being applied through the characteristics  
14 inside your Web browser.

15 And what you'll see is that you get different  
16 measurements of bits of information from different things  
17 like the operating system version, or the browser  
18 version, or the fonts on your computer. And for a lot of  
19 people right now their browsers have enough independent  
20 bits of information to essentially be like PII.

21 If you attach it to a name, you know, it's a  
22 fingerprint that you can take around the Web with you and  
23 leave it everywhere, and all your actions can be  
24 correlated with it.

25 MS. GARRISON: Anne, I want to throw a question

1 to you that's related to this. Should we care whether  
2 data can effectively be identified, or should we change  
3 consumer expectations and accept that there is ubiquitous  
4 collection of all information about us, no matter the  
5 source, whether it's publicly available or privately  
6 held?

7 MS. TOTH: On the deidentification side, I  
8 mean, certainly, as a company that's engaged in search --  
9 and there are other notable companies in the audience  
10 today that are engaged in search -- we have taken a  
11 number of steps to deidentify search data. And in our  
12 case, you know, all log file data, it's -- as a business  
13 you are, you know, while -- if you take Arvind's argument  
14 that, you know, to the nth degree that eventually in some  
15 way, shape, or form all bits of data are personally  
16 identifiable if you associate them with one another, and  
17 I think technology certainly removes some of the  
18 boundaries.

19 I mean, with the pace of technological change  
20 it's entirely possible that you could make that argument  
21 that as a business you are definitely going to have  
22 different types of security systems for systems that  
23 store credit card information than you are systems that  
24 store aggregated demographic information, for example.

25 So there are going to be pragmatic differences



1 in how you treat data, because I think not all data are  
2 created equally. And we are going to take steps to  
3 deidentify data, but they have to be coupled with really  
4 strong data policies because, as we have all discussed  
5 here, technology makes it, at the rate of change, makes  
6 it very hard to say that you could never do something  
7 because certainly if you have enough time, enough  
8 engineers, enough money, enough access to other databases  
9 that exist in the world, there is a lot of things that  
10 you could do.

11 I've said before, in our privacy policy we  
12 state a lot of the things that we do do, what we do with  
13 data, but it would be impossible to write a policy that  
14 lists out all the things I don't do today. I don't eat  
15 small puppies. I could put that in there. But I mean,  
16 it's sort of -- it's just that there is an infinite list  
17 of things that you don't do.

18 So I think that from a pragmatic standpoint as  
19 businesses we have to make decisions based on resources  
20 and what's practical to do. So that's an important  
21 consideration. I just want to make sure that we think  
22 about that. I think there are lots of -- when I read a  
23 lot of these articles I think they are fascinating, but I  
24 also know that, you know, we have strong policies in  
place to do the best we can to prevent, but policies in

160 TD678 things from opposing sides. 24040 TD (b) (5) d. 24040 TD (b) (5) d. 24040 TD (b) (5) d. 160 TD678 things ffffffff Now, in terms of ubiq

1 hearing from me and when they walk out of this room what  
2 they think about me, certainly. So there are some  
3 natural limits to that.

4 MS. HARRINGTON-McBRIDE: I just have a brief  
5 announcement. There is apparently a two-door, red,  
6 Toyota Camry parked behind the law school, but you didn't  
leave the keys. So if thatEalyli of thi diertould0 TD eP-2.2ruwe TD ra-TON-Mc2.2678eThear -2.28f9ahat

1 that very broadly, but were to shed that data within 24  
2 hours I think some of the privacy risks may be  
3 diminished.

4 I think some of the risks that we all think  
5 about and theorize about and see in actual practicality  
6 increase as data is held and combined over time. I think  
7 something else that could be of practical help is the  
8 role of privacy audits on what companies are doing with  
9 the data.

10 And we really don't talk enough about that  
11 aspect of companies having third-party, independent,  
12 privacy audits that are published on how they are  
13 managing data, and put those out for the consumer.

14 MS. HARRINGTON-McBRIDE: All right. We are  
15 going to continue our discussion now with some of the  
16 issues related to privacy-enhancing technologies, and  
17 start to look at some of the ways that technology can be  
18 used in ways that may help protect consumers' privacy,  
19 and also finally get to this question that I think  
20 everybody's been wanting to answer and been starting to  
21 answer, which is, what role do businesses play and  
22 organizations generally, not just businesses, play in  
23 helping to protect consumer privacy, and how can they use  
24 these technologies wisely.

25 So with that, what are the tools that have been

1 developed to date? Let's talk a little bit historically  
2 about ways that technology tools have been developed to  
3 give consumers control to allow them to manage the  
4 collection or use of their data. Any historians on the  
5 panel who want to take a shot at this, or shall we do it  
6 as a Wiki?

7 Eric.

8 PROFESSOR GOLDMAN: Well, I'm not sure I'm  
9 going to answer your question directly, but I think maybe  
10 we can take a cut at it by trying to define what we mean  
11 by privacy-enhancing technology, because I think a lot of  
12 times when we have these types of discussions people  
13 default to think, oh, we are talking about P3P again.

14 And we should talk about P3P. It is a prime  
15 example of an effort to establish some type of  
16 privacy-enhancing technology online. But I think a  
17 privacy-enhancing technology is anything that can help  
18 consumers manage their information flow. So in my mind,  
19 when I think about antispam software or antispam filters,  
20 -- in my mind -- that's a privacy-enhancing technology.

21 When I think about antispyware software or  
22 antivirus software, that is in a sense a  
23 privacy-enhancing technology. It might have other  
24 benefits, as well. It might also enhance security, but  
25 it fits into the same bucket. It's managing the

1 information flow.

2 And I don't mean to speak for Yahoo!, but

3 perhaps we might even go so far as to say that the

4 privacy manager systems that you guys offer would fit

into the brTTTTTTTTT sfar as to say that the

1 educate consumers in a consistent way across the industry  
2 that when you receive an ad online you can go and look at  
3 this icon, click on this icon and find out ultimately --  
4 and this is the direction we are moving in is actually --  
5 by transmitting some meta data about the ad with the ad.

6 A user can some day in the very near future be  
7 able to see who's serving that ad to me, where can I go  
8 to opt out. And when the user goes to opt out at that  
9 point we can actually show them, we at Yahoo! do show  
10 them, this is what we are using to customize your  
11 advertising; this is how you can interact with this;  
12 these are the categories you can turn off; you can turn  
13 them all off.

14 In our view it's really about simplifying this  
15 for consumers, because there is so much here that we are  
16 talking about and it is complex, absolutely. And  
17 technology is moving at a pace that it's only going to  
18 get more complex.

19 So how do we simplify the choices and give  
20 people, really, access to what is important to manage and  
21 give them, certainly, the flexibility and the granularity  
22 of controls without completely overwhelming them with so  
23 much information about information.

24 That is, I think, our challenge. And we are, I  
25 hope, stepping up to the plate and providing one model

1 for how that can be done.

2 MS. HARRINGTON-McBRIDE: All right. Before we  
3 go any further, does anyone on the panel have any  
4 thoughts about the definition that Eric has drawn for us,  
5 which is a very broad and expansive one? Should we be  
6 thinking that broadly about what constitutes a  
7 privacy-enhancing technology?

8 Does anyone take issue?

9 Peter?

10 MR. ECKERSLEY: I don't know whether this is a  
11 definition, but the best way I think to think about  
12 privacy-enhancing technologies is that they are about  
13 putting the genie back in the bottle in general. What  
14 tends to happen, the points got made earlier on, is that  
15 the privacy threats come from the design of technologies,  
16 and the design of technologies not necessarily to invade  
17 privacy but, really, just to make them as feature-full as  
18 possible.

19 So one example of that is the Web. And if you  
20 look at the Web and the privacy threats that we find in  
21 the Web, they start with IP addresses, which were  
22 necessary to make TCP connections, to fetch data from a  
23 Web server. They include the third-party content that  
24 can see what you are doing, which came from the desire to  
25 make the Web a hypertext system, so that content from



1 different places could be combined.

2 They include cookies, which were designed to  
3 make the Web a stateful user interface so that Websites  
4 could remember that you had pressed a button previously.  
5 They include Javascript, which was intended to make pages  
6 do things that are more like computer programs and less  
7 like flat text documents.

8 They include Flash, which was intended to embed  
9 moving images, and animation, and interacting animations,  
10 and pages. So each time we added a new feature we  
11 created a new privacy threat. And what privacy-enhancing  
12 technologies are doing is they are trying to run around  
13 after all of these new features. And their task is very  
14 hard because the feature, if you just block the thing you  
15 have lost the feature. You are browsing the Web like  
16 it's 1990 again.

17 And so what you are trying to do, if you are  
18 building a privacy-enhancing technology, is put the genie  
19 back in the bottle, except occasionally you want the  
20 genie because it's cool and it grants you wishes.

21 And the technology needs to know the difference  
22 between the good genie and the bad genie. And I think  
23 that's fundamentally why privacy-enhancing technologies  
24 are always losing this arms race and why, perhaps, we  
25 need to break that circuit somehow.

1 MS. HARRINGTON-McBRIDE: All right.

2 Sid.

3 MR. STAMM: I want to add that I believe that  
4 it's more than one genie in this bottle. And I think  
5 what we should do is not only run around and try and put  
6 the genie back in the bottle afterwards, but also allow  
7 people to know about this fire hose of features that is  
8 the Web, and turn off the ones that they are personally  
9 worried about.

10 So our philosophy is that privacy matters and  
11 people like to be able to opt out of these things. And  
12 so in Firefox, for example, we have been making it  
13 central that the user can control all the data that goes

1 with Sid that there is a lot of genies. We have been  
2 talking so far about privacy-enhancing technologies that  
3 really empower the consumer, and those are critical. But  
4 you know, if we think about concepts that Anne and others  
5 have brought up -- Chris -- around organizational  
6 accountability, the fact that technology alone isn't  
7 going to solve the problem, that companies are going to  
8 have to be accountable, I think we need to think about  
9 privacy-enhancing technologies in how they can be  
10 employed or deployed inside of organizations that are  
11 actually having to make decisions about these  
12 technologies and about the uses of data.

13 So I think that it's not just what we can  
14 provide to the consumer to empower them, to provide  
15 controls for them, but how we can use technology to  
16 ensure that the commitments and the policies that we put  
17 in place as an organization and the promises that we make  
18 to our data subjects, that there really are  
19 implementation mechanisms and assurance monitoring, that  
20 we are upholding the promises that we make. And as a  
21 large organization we certainly use technology to help us  
22 implement those promises and ensure that we are upholding  
23 those promises.

24 So I think that privacy by design, as  
25 Commissioner Harbour was talking about earlier, comes in

1 many forms, not just for the end user, but for  
2 organizations themselves to help make sure that they do  
3 what they say.

4 MS. HARRINGTON-McBRIDE: Pam.

5 MS. DIXON: Yes. There is a couple of thoughts  
6 here. I think that your point is very interesting,  
7 Scott. I think that there is a really good role for  
8 privacy-enhancing technologies in business processes.  
9 And what comes to mind, of course, is the credit  
10 reporting industry and also the pervasive scoring  
11 industry, you know, your identity score, your fraud  
12 score, your anonymity score. And there's algorithms that  
13 could be managed by certain technologies, and whatnot.  
14 But also in the offline world I think we need to think  
15 about privacy-enhancing technologies. I mean, we have  
16 been talking about the Web a lot.

17 So on the Web we have opt-out cookies. But if  
18 you are walking in a public space your opt out cookie is  
19 a pair of sunglasses, you know. So this is a -- where do  
20 the privacy-enhancing technologies come in for that or  
21 for commercial data brokers when you end up on the sucker  
22 list?

23 There needs to be some kind of business process  
24 that has a privacy-enhancing technologies that enforces  
25 consumer preferences and fraud policies.

1 MS. HARRINGTON-McBRIDE: I want to hear from  
2 Chris and Arvind, but I want to follow up on a note that  
3 seems to be coming through a lot, which is there are a  
4 lot of genies. I think we have a lot of things here, a  
5 lot of genies, a lot of silos, a lot of organizations  
6 doing the collection and a lot of means that consumers  
7 may need to know about to enhance their privacy-using  
8 technology, all of it making a very complicated  
9 ecosystem.

10 Is there any sort of killer app in the pets  
11 world that could holistically change this? Are there any  
12 -- could there be such a solution?

13 DR. NARAYANAN: The basis on which to  
14 understand privacy-enhancing technologies is who is the  
15 target audience. And the economic study of privacy has  
16 given us some great insights on this. It divides  
17 consumers into pragmatists and the other five percent of  
18 the people who are really concerned about privacy.

19 If you look at the history of privacy-enhancing  
20 technologies it's been really successful for that  
21 five-percent minority, but not so much for what  
22 economists call this pragmatic majority. And good  
23 examples of both of those would be, I'm again going to  
24 bring up Tor, that's only a small percentage of the  
25 people who are in a sufficiently privacy critical

1 situation to go to the extent of installing and using  
2 Tor. And it's done a great job for them.

3 If you look at a technology that's meant to  
4 help this majority, a good example would be Facebook's  
5 privacy settings. Now, even when they had, you know,  
6 fairly sophisticated privacy settings before and even now  
7 that they have simplified it a little bit, in both of  
8 these instances we find that, you know, the percentage of  
9 users who are again going to the trouble of dealing with  
10 these settings is fairly small.

11 And so that segues into the question that you  
12 asked, which is that is there going to be something  
13 that's sort of like a silver bullet that's going to  
14 tackle this holistically. I'm getting the sense that the  
15 answer is probably not, because that would require  
16 something, you know, that the average person can use.

17 And in terms of this tradeoff between usability  
18 and enhancing privacy, we have not done so well. So we  
19 are always going to continue to see really good solutions  
20 for that five percent, but for the 95 percent it's going  
21 to be troublesome.

22 PROFESSOR HOOFNAGLE: I think my comment  
23 follows yours nicely, Arvind.

24 Katie, you started this vein of questions by  
25 invoking the history of this issue. And I think one of

1 the things that's worth looking at is the 1996 staff  
2 report, which discusses self, which discusses PETs in  
3 detail. And I doubt any of us could even name the PETs  
4 that were on the table back then, but they included  
5 predecessors P3P.

6 Cookies were considered a type of  
7 privacy-enhancing technology, and a content filtering was  
8 considered as one of them. But the point I wanted to  
9 raise was that at the '95 workshop I think the most  
10 prescient comment in any of the workshops that have  
11 happened was made by Beth Givens.

12 She said back in '95, whatever you do, create  
13 benchmarks; come up with some standard questions, some  
14 standard goals, and ask yourself every year, are we  
15 reaching these goals. I think with PETs we could agree  
16 upon some consensus standards to see whether we are  
17 moving forward or backwards.

18 They would be things like: Are consumers aware  
19 of privacy-enhancing technologies? How much adoption are  
20 there of them? Arvind mentioned the magic five percent.  
21 Does it ever leave that five percent? Do the available  
22 PETs actually address the threat landscape, is another  
23 benchmark that could be analyzed.

24 Are these PETs usable and can people with a lot  
25 of incentives, ad networks, et cetera, to undo those

1 technologies, are they able to circumvent PETs? If we  
2 started out with some benchmarks here we could come back  
3 to the next roundtable five years from now and we could  
4 say: Have we made any progress or not?

5 MS. HARRINGTON-McBRIDE: Sid.

6 MR. STAMM: I think you're exactly right. I  
7 think that one of the good success stories in getting  
8 privacy-enhancement technologies adopted is cookies. And  
9 people are now really aware of cookies and a way larger  
10 proportion of people clear their cookies on a regular  
11 basis now.

12 And although we might not be able to come up  
13 with a silver bullet like Arvind was talking about, I  
14 think we can at least come up with, you know, maybe a  
15 partially silver hammer that makes it easier for users to  
16 address a lot of privacy concerns in one shot.

17 This is one of the approaches we are taking  
18 with our privacy manager in Firefox, is we want to make  
19 it as easy as possible for users to understand how much  
20 private data is on their browser that's being sent out  
21 and wipe it out if they want. And we have kind of been  
22 slowly moving in that direction.

23 MS. HARRINGTON-McBRIDE: Well, I think that  
24 that's an excellent point and, not coincidentally, you  
25 are here representing a browser company. Let's examine



1 the question.

2 If we have, as Arvind has pointed out, perhaps  
3 95 percent of the folks out there who are encountering  
4 technologies in an online space and not even to get into  
5 the offline just yet, who are unaware of what they may  
6 need to do, or unwilling because of time constraints or  
7 knowledge restrictions to engage with this, what are  
8 better solutions?

9 And it seems to me that everybody needs a  
10 browser. So are browsers a place where some of this  
11 should be happening; should there be -- you know, what's  
12 going on in the marketplace today and can more be done?

13 MR. ECKERSLEY: Well, I think one of the  
14 reasons why browsers are particularly important, at least  
15 if we are talking about the Web, which is one important  
16 domain, there are others, the reason browsers are  
17 important is because they wield the incredible power of  
18 defaults.

19 If your browser does something for you, then  
20 that's suddenly there for 95 percent of people. Whereas,  
21 if it's a thing you need to go and install, if it's an  
22 extension or a plug-in, a buried setting, then you are  
23 talking five percent at most. And so that's the one real  
24 thing we need from browsers.

25 Now, look, there is a structural concern, I

1 think, which is that of the major browser manufacturers,  
2 I think maybe there are four of them, three and a half of  
3 those are funded by advertising revenue, realistically.  
4 So I think -- I mean, of course, the browser  
5 manufacturers will tell us, no, no, that that doesn't  
6 change our engineering decisions.

7 But the reality is, probably, it would be  
8 really hard for them to take very strong privacy  
9 protective steps because it undermines the business  
10 models that fund them. So I think this is a hard  
11 question to answer, but we need to confront it and talk  
12 about it.

MS. HARRINGTON-McBRIDE: Okay. Eric.

1 each of those, whoever we pick here, is what regulatory  
2 overlay will apply to.

3 So, for example, you may recall the battles we  
4 had in the 1990s over what could be integrated into the  
5 operating system, or what had to live in the browser.  
6 Those types of questions actually might steer the answer  
7 to the question that you are asking.

8 MS. HARRINGTON-McBRIDE: Thoughts on that,  
9 Anne?

10 MS. TOTH: I just wanted to point out consumer  
11 attitudes vary a lot and consumers are fascinating  
12 creatures. You have a small percentage who care  
13 incredibly deeply about personal privacy and then you

est 6y,bcams







1 this morning. And for that I will turn to Lori.

2 MS. GARRISON: I want to pick up on Scott's  
3 point about the need for accountability, or how  
4 accountability not only helps consumers in terms of  
5 understanding where the data flows, but it's also  
6 important to businesses. Can you talk a little bit more  
7 about that, especially historically?

8 I think you had mentioned at one point that ten  
9 years ago businesses knew who they were dealing with,  
10 knew where the information came from, where the  
11 information was going. There were contracts among all  
12 the parties. Everybody had certain expectations. It was  
13 relatively easy to audit. But the world has changed  
14 pretty dramatically.

15 And, in fact, you have less control and less  
16 knowledge, at least from what you had explained from a  
17 business perspective about what is actually happening in  
18 this environment.

19 MR. TAYLOR: I think that what I probably  
20 mentioned was that ten years ago or in the early stages  
21 or even before the Internet, information sharing was very  
22 different. Collecting of information, generally, the  
23 consumer understood the brand that they were interacting  
24 with, and that brand was able to make promises.

25 They were able to determine whether that brand

1 was reputable to them, and that gave them a lot of  
2 comfort. They knew who to go back to if there was a  
3 problem. Sharing of information back then was much  
4 easier because, you know, you generally had big tapes  
5 that had information. And you knew who you were giving  
6 them to and you were able to easily put contractual  
7 agreements in place so that that third party understood  
8 the obligations of the primary brand.

9 In a network Internet world where I think about  
10 network affiliate advertising, which is the lifeblood of  
11 many organizations to be able to advertise and target  
12 information, information is flowing so many different  
13 places. And you may have agreements and understandings  
14 with the next person in the chain of accountability, or  
15 as Commissioner Harbour said I think the chain of  
16 custody.

17 But where does that information go beyond that?  
18 And I think that was my point, of it's becoming harder,  
19 even for a primary brand who is wanting to be transparent  
20 and explain exactly how data flows and what third party's  
21 data may go to, it's just becoming more and more complex.

22 And I'm not sure that we have revisited how we  
23 ensure that that chain of accountability is actually  
24 achieved, and how you can ensure that when data flows to  
25 you that you understand where that data came from and the





1 to come out of a reticence risk.

2           Whereas, if we were able to deploy technology  
3 -- and I think Chris started to touch on this, and  
4 earlier, Arvind was wanting to talk about it. If you can  
5 imagine that -- that we have a framework from regulation  
6 or industry codes of conduct that help us to understand,  
7 let's say, use categories and the obligations and consent  
8 that people give around the use of their data.

9           If technology were deployed through tagging, as  
10 Anne said, and that followed the data, certainly, that is  
11 going to not only provide better consumer protection, but  
12 it will ensure that organizations where data flows to us  
13 or where we flow data out, that it's understood what  
14 those obligations are.

15           And I actually think that that will not only  
16 help to improve protection on the part of consumers and  
17 some redress, but it's also going to help to ensure that  
18 information can be used robustly, but that organizations  
19 can demonstrate accountability and responsibility as they  
20 use that data.

21           MS. HARRINGTON-McBRIDE: Pam.

22           MS. DIXON: I think one of the issues -- I  
23 appreciate your point, and I think I've thought about  
24 those a lot -- but one of the real down sides of this --  
25 it's kind of like identity theft. Identity theft was a

1 real boon to the privacy argument, but the downside of  
2 identity theft is all of a sudden you get all of these  
3 really invasive authentication techniques.

4 And this is the same downside with what you are  
5 proposing. The tagging of the data is good, but for  
6 consumer accountability you are really going to have to  
7 have some kind of authentication of that consumer to some  
8 degree, and in some kind of constructs of how this could  
9 be deployed.

10 So I think that if that is a concept that's  
11 followed through, we are going to have to be very, very  
12 careful about how the consumer and if the consumer needs  
13 to be identified in order to have some accountability  
14 here. I think if we are looking at a world in which all  
15 the data is tagged and then tied back to the identity of  
16 a consumer, I think we are looking at less privacy rather  
17 than more and we have got to be really careful of that  
18 authentication issue; yeah.

19 MS. GARRISON: Chris, are we looking at less  
20 privacy? In fact, are we getting to your data provenance  
21 so that it may be easier for consumers to be able to  
22 access their data and be able to make corrections at the  
23 source of the data collection.

24 PROFESSOR HOOFNAGLE: Some of that -- I think  
25 some of the legal infrastructure is already there. So

1 for a long time in the offline and increasingly in the  
2 online world major list houses have used contract to  
3 promote accountability. And if you get any of those  
4 contracts you'll see that they are -- they often follow  
5 fair information practices.

6 They require buyers of data to only use the  
7 data for certain purposes, to delete it after they have  
8 used it for their marketing campaigns, et cetera. But  
9 there is also some kind of secrecy norms that are built  
10 into them. So, for instance, you'll see that some list  
11 houses will say, don't tell the consumer where you got  
12 this information.

13 Or let's say you bought a list of people -- and  
14 this is a real example -- let's say you bought a list of  
15 people who have incontinence problems. You are not  
16 allowed to tell the consumer where that list came from or  
17 the fact that you know about their medical problems, but  
18 then you can send them some type of marketing material.

19 And when you look at these contracts you'll see  
20 that they even include provisions for breach notification  
21 from marketing data that is not subject to state  
22 notification law. So there is a lot of at least paper  
23 accountability there. I think the problem comes back to  
24 incentives.

25 Enforcing one of these contracts would shine a

1 light on your data sharing and it would shine the light  
2 on the fact that you have sold data to a company that  
3 used it inappropriately. So I think there is still a lot  
4 of work to do up there on the legal front, but let me say  
5 it again.

6 I think it's important to note that when these  
7 companies use private ordering to create accountability,  
8 their private ordering looks like fair information  
9 practices.

10 MS. GARRISON: Scott, did you have a comment on  
11 that or a response?

12 MR. TAYLOR: No. I just wanted to comment that  
13 I don't disagree with Pam that the concept I came up with  
14 is not a simple thing to implement. The point is that as

13 s 12 108415 0 TDsimpl

1 appropriate information and obligations flow with data in  
2 the future.

3 MS. GARRISON: I just want to make an  
4 announcement for folks who are using the Webcast. If you  
5 are having problems please reload the Webcast and then it  
6 should function properly. On the issue of consumer  
7 preferences, because the data, as I understand it, the  
8 data tagging would not only include the provenance of the  
9 data, but would also incorporate consumer preferences.

10 How far down the line, down the chain of  
11 sharing, what -- should those preferences go? In other  
12 words, if -- if I deal with Company A and I say, I don't  
13 want you to share my information with your affiliate or  
14 with these third parties, how can that be honored down  
15 the chain as the information -- because once it goes out  
16 the door it goes everywhere. Can you address that, or  
17 anybody else?

18 MR. ECKERSLEY: I'd just point back to that  
19 idea of reviving the fair information practice of access.  
20 I mean if it's gone down the chain and there is an  
21 efficient way that the subject of that information can  
22 see that that happened, then perhaps we could talk about  
23 what kind of recourse they might have. Until you know  
24 that it's happened it's really hard to imagine an  
25 enforcement regime that does anything about it.

1 MS. GARRISON: But, technically, is it feasible  
2 to have that information in the tag so that it's known  
3 and could be traced all the way through? Do you know,  
4 Peter? or Arvind?

5 MR. ECKERSLEY: I mean it's a very general  
6 question, but I think if people are prepared to do the  
7 engineering work then, yes, you can tag data. In  
8 practice it may be more complicated in particular  
9 industry sectors or in particular systems but, in  
10 general, the answer should be presumed yes, until shown  
11 otherwise.

12 MS. GARRISON: Eric, you had a comment?

13 PROFESSOR GOLDMAN: Yes. I'm going to try and  
14 explain why I don't have an answer to your question, and  
15 perhaps why maybe we don't. Perhaps I'm being overly  
16 cynical about this, but it seems like somewhat of a lost  
17 cause to think about trying to establish a truly rigorous  
18 consumer-managed experience about this flow of data  
19 outside of their purview.

20 I mean I don't even understand how to frame  
21 that discussion in an intelligent way. It points, in my  
22 mind, to the need to really think about how the consumers  
23 can control their own experiences when the data comes  
24 back to them. In other words, I don't care so much about  
25 if people are sharing my email address among all of them

if I never see the email that comes from it.



1 the bottle, I think is the metaphor that's been overused  
2 and in the end, ultimately, let's start with some  
3 premises.

4           You know we talked a little about picky  
5 defaults, that defaults, or whatever the computer system  
6 is, matter. But I think the problem is far more  
7 pervasive than that. Computers are really complex  
8 animals and it's unrealistic to expect that consumers  
9 will understand how their computer works, understand how  
10 other peoples' computers work, and then be able to figure  
11 out how to put that all together in a way that it  
12 optimizes their experiences for themselves.

1 discussing here, so much of this seems to me to be  
2 solvable only at the clients' side, not anything that we  
3 can do at the other end of the system, with all the  
4 different people who are trying to slice and dice data to  
5 try and come up with a better crafted message for some  
6 other person, or engage in some kind of security threat,  
7 it's that we need good shields at the consumer level.

8           And we need to make sure that we have a system  
9 that enables those technology providers to do the things  
10 that they -- consumers want them to do, knowing the  
11 consumers will never fully understand what they are  
12 doing, and are okay with that.

13           MS. GARRISON: Arvind.

14           DR. NARAYANAN: I just have a data point to add  
15 to that. I was talking to a personal genetics company  
16 recently and they said that their policy is that each  
17 time they share their data with a new partner the  
18 consumer has to reauthorize that. And so clearly they  
19 felt that it's feasible to sort of bother the consumer to  
20 do that, and also that technologically there is no  
21 problem in achieving this.

22           So I think it boils down to a question of  
23 incentives. Genetic data is viewed by consumers as very,  
24 very sensitive information and, therefore, this company  
25 felt that the proper thing to do was to have this

1 reauthorization mechanism. So I think there is a role  
2 for very strong controls on where data is flowing.

3 We also, as Eric mentioned, for some kinds of  
4 data like my email address, I don't want to keep doing  
5 that every single time. So we have to look at a spectrum  
6 of different solutions.

7 MS. GARRISON: Pam.

8 MS. DIXON: Yes. You've touched on an  
9 important point, which is the role of authorization or  
10 consent being very different items. I think one thing  
11 that usually comes up in these kinds of discussions is,  
12 oh, well, let's have the consumer consent and that will  
13 really carry the privacy water.

14 And I think one of my pet peeves is that we  
15 have got to be really careful about how we build consent  
16 into any kind of privacy-enhancing technology system,  
17 because consumers will just click on anything. And this  
18 is not ultimately a good privacy protection for them. So  
19 I would just urge caution in thinking about that.

20 MS. GARRISON: Well, I think we have come to  
21 the end of our discussion. I want to simply close with  
22 saying that we have the Chief Privacy Officer of Adobe  
23 who is attending today, and because we did talk about  
24 Flash cookies in the beginning, to announce that Adobe  
25 has filed a comment which should be up on our Website



1           PANEL 2: PRIVACY IMPLICATIONS OF SOCIAL NETWORKING  
2                    AND OTHER PLATFORM PROVIDERS

3           MR. MAGEE: Good morning, everyone. My name is  
4           Peder Magee, and with me is my Comoderator Michelle

1 questions of the panelists. We encourage everybody to  
2 participate. If you'd like to be recognized, please turn  
3 your table tent to the side.

4 MS. ROSENTHAL: I'll just remind everyone that  
5 if you

6 have questions, you should have question cards in your

folders. Someone will be walking around to collect your

7 have questions, you should have question cards in your folders. Someone will be walking around to collect your questions. We encourage you to submit questions in writing if you have any. Thank you.

1 you to the FTC for the invitation to come and address all  
 2 of you and share in this conversation.

3 We at Facebook feel that there is extraordinary  
 4 value, and I think it's now unassailable, to having  
 5 people have the opportunity to connect with people at any  
 6 moment at any time anywhere in the world, as long as they  
 7 have access to the Internet.

8 There are a myriad of new goods and services  
 9 which have been brought to bear, not just by Facebook, by  
 10 other social networks that came before us, others that  
 11 will come after Facebook and others that are sort of  
 12 niche players in this market. And I think people forget  
 13 that there are, you know, by some counts 20 different  
 14 social networks around the world and Facebook is just one  
 15 of them.

16 So it's hard to speak to the entire  
 17 marketplace, but on our behalf, we feel that at least  
 18 amongst our users they have found extraordinary value to  
 19 being able to contact people and share experiences about  
 20 their lives, their thoughts, the things they are seeing

13 about 2415 wedpeukught to 4 different  
 2415 wedpeukught to 4 different

1 MR. MAGEE: Erika.

2 MS. ROTTENBERG: I echo precisely what Tim said

3 and thank you very much for the opportunity to speak.

4 What I'd say is that since Adam and Eve, people have

5 wanted to connect. And you go back to the shtettles of

6 Europe, and people connected within their shtettle.

7 You think about the Model T Ford. And people

8 expanded their reach and started to connect with people

9 who live a little bit further away. I used to live in

10 Alaska and there are villages that were snowed in. And

11 what did people do?

12 They used what was called RapNet, which is, you

13 know, the old, you know, basically radio show. And you

14 would call in to be able to do communications with people

15 who lived in villages that were shut off because of the



1 online professional identity that broadcasts to those  
2 whom that individual user makes a conscious decision to  
3 whom it is they want to broadcast that to, whether it's  
4 just to their connections, whether it's their connections  
5 of their connections, or whether it's to the LinkedIn  
6 community at large.

7 We look at, and our mission statement is, to  
8 connect the world's professionals to make them more  
9 productive and successful. The number of emails that we

1 to California and bringing us sun for the first time in  
2 two weeks. So thank you for that.

3 I was actually really pleased to be on this  
4 panel, although like for the formal, social network that  
5 Google has, which is really most important to people in  
6 Brazil and India, and probably relatively nonexistent for  
7 anyone in this room, I was suddenly, well, what am I  
8 doing here.

9 But the fact of the matter is, the nature of  
10 social media, which Google does participate in, is  
11 permeating all types of platforms. And why is that so  
12 important? I think it's about sharing and collaboration  
13 and really harnessing the promise of the Internet, which  
14 is reach, and reach at a global level.

15 So as just one concrete example of, like, why  
16 does that make a difference, one of the things we did  
17 last night on YouTube is we had President Obama's State  
18 of the Union broadcast live through CitizenTube. We  
19 combined that with Google moderator so that users could  
20 go and ask a question, which President Obama will answer  
21 live in a YouTube broadcast next week.

22 The Google moderator basically takes in  
23 questions and then users vote about what, was that a good  
24 question, you know, like let's ask that one for sure.  
25 And what we got as of -- I checked -- midnight last

1 night, we had 287,000 votes on over 7,000 questions from  
2 almost 30,000 people.

3 The nature of that sort of participatory  
4 democracy is something that we have not seen, other than  
5 in small town halls in small communities, in a long time,  
6 and we can do this at a national scale. And I think that  
7 is the promise of what social media can bring.

8 So those are the things that I think we are  
9 only starting to see the edge of. Just sort of thinking  
10 through, like, social-networking service, can we define  
11 it, I think it's often been defined in closed systems.  
12 But, as I was saying, I think we are now starting to see  
13 social move into the open Web.

14 We are having trouble defining what social  
15 media means because it is still evolving, and this is a  
16 great panel to start thinking through what our  
17 expectations of those medias are.

18 MR. MAGEE: Thanks. I want to -- since this  
19 also about other platforms, I want to ask Ian if you  
20 could talk about some of the benefits associated with  
21 third-party applications that ride on top of platforms.

22 MR. COSTELLO: I think, kind of tying into  
23 what's been said, that with all this hyper connectivity  
24 people also not want to just connect, but try new things.  
25 People are really drawn to innovation, and with opening

1 up these platforms and creating very, very low barriers  
2 to this innovation, it just continues to give people new  
3 things to try.

4 Maybe they'll download an iPhone app. Maybe  
5 they'll love it or maybe they'll delete it but, again,  
6 it's that ability to try that's important, and that  
7 opening up kind of enables and it drives this kind of  
8 virtual cycle of more and more people demanding more and  
9 more kind of things to try, which creates kind of the  
10 room for developers to move in and do that, and that that  
11 demand is creating, as we have seen with Google,  
12 Facebook, LinkedIn, Apple now with the Tablet.

13 Just last week I think we are hearing that the  
14 Amazon Kindle is opening up to developers. So, again, we  
15 are seeing a tremendous market movement towards opening  
16 up platforms for third-party apps, and that's what I  
17 think is just validating a lot of the value for  
18 consumers.

19 MS. ROSENTHAL: So I think it's clear that  
20 there are benefits to social-networking sites and  
21 platforms and applications, but maybe we can talk a  
22 little bit about the risk of harm to consumers that are  
23 created in this space.

24 Things like photo and video sharing, there is  
25 lots of sharing of information online, and it might be

1 helpful to consider sort of how this space differs from  
2 the offline space and whether it differs from the offline  
3 space. Lots of personal data is being uploaded every day  
4 and great numbers of people are able to access that data.

5 And so given this what are the harms that we  
6 are concerned about? Is it simply embarrassment or  
7 chilling of a consumer's participation in a beneficial  
8 network that something they might benefit from, yet they  
9 are not actually participating because they are concerned  
10 about their privacy.

11 Lillie, do you have any examples of some of the  
12 harms or the risks?

13 MS. CONEY: Yes. First, I wanted to wish  
14 everyone a happy and productive International Privacy  
15 Day. I thank the FTC for selecting this day for these  
16 series of discussions. EPIC routinely communicates with  
17 the FTC about matters that effect consumer privacy  
18 rights.

19 We do this because of the interest of the  
20 organization in making sure that those harms or those  
21 negative impacts are addressed in the way that will be  
22 most beneficial to them. We are not the only  
23 organization that works in this area to bring to the  
24 attention of agencies, to provide services or benefits to  
25 consumers.

1           Joining us in a lot of the work that we do, the  
2           ACLU, EFF, Consumer Privacy Rights Clearinghouse, as well  
3           as Consumer Watchdog, are all vital partners in this work  
4           that we do. The impacts to consumers are varied, but the  
5           specific issues that we look at around social networking,  
6           -- there was a report in July of last year of a  
7           cheerleader who sued her coach.

8           The coach requested the cheerleader's logon and  
9           password for her Facebook page which he got, looked at  
10          the page and then shared content with school officials  
11          who later sanctioned the cheerleader because of the  
12          content on her page. This isn't just something that  
13          would happen to a young person.

14          We have Bozeman, Montana, that had a job  
15          application that required applicants to provide their  
16          logon and password for social-networking sites, and what  
17          they said was basically for background check purposes.  
18          We have had circumstances where the researchers at  
19          Carnegie Sci Lab who looked at social security numbers  
20          and the master death records and basically proved that  
21          the information provided by social network users, the  
22          basic logon information, name, location of birth, date of  
23          birth, they could use that information to literally guess  
24          the last four digits of individuals' social security  
25          numbers, which are very relevant for identity theft,

1 which is one of the issues regarding how social-  
2 networking services provide content to other users.

3 We also have cases where there was a research  
4 project at MIT that basically stated they could guess the  
5 sexual orientation of individuals who were linked through  
6 social-networking services. Whether this is borne out  
7 through research or not, the fact that that was something  
8 that a research project could pursue and then later  
9 provide some definitive statements regarding opened up  
10 the possibilities of what some of the harms or potential  
11 harms could be to social network users.

12 MS. ROSENTHAL: Thanks, Lillie.

13 Chris.

14 MR. CONLEY: Actually, I'm going to follow up a  
15 little bit on that research project, because that's what  
16 I want to talk about. A few things have changed with  
17 social networks going from the water cooler or the coffee  
18 shop to the online world. And the biggest thing is that  
19 the information has changed.

20 It used to be if you are in a coffee shop, the  
21 people who know you are there are the other people in the  
22 coffee shop. Now it's anyone who can see your profile.  
23 That information is permanent. If you spoke to someone  
24 online, there is a record of that and there is a  
25 connection, a list of your friends that anyone can access

1 at any time.

2 They don't have to see you with people. They  
3 can look at it. It's very easy to take around. It's  
4 very easy to share with other people, share with other  
5 companies, to look around. And it's also very easy to  
6 aggregate and do very interesting things with, and that's  
7 where this research project comes in.

8 The MIT research project is called Gaydar, and  
9 essentially all it did was look at the social graphs of  
10 who your friends were. It looked at their gender and  
their sexual orientation and it tried to figure out how likely they were to be gay or lesbian.

their orientation and likely to figure out their sexual orientation and likely to figure out



1 the long-term consequences. They only think about the  
2 short-term benefits. So are minors at a greater risk in  
3 this space? You know, is this something that we should  
4 be concerned about? Do they -- are there other things  
5 that we should be worried about that maybe don't apply to  
6 adults?

7 Lillie?

8 MS. CONEY: Minors, the relationships that  
9 minors create on social-networking sites initially only  
10 involved other minors. The original -- or young people.  
11 The original focus was online campus communications at  
12 Harvard and it began to grow beyond that.

13 The social-networking norms or activities of  
14 children or young people online evolve over time. If you  
15 ask a young person -- the question is not about whether  
16 they care about privacy or not. That's too generic. Ask  
17 them questions about, would you friend your mother; would  
18 you friend your father; would you friend your  
19 grandparents; would it be okay if they saw the content on  
20 your page or the IM messages you were sending. You will  
21 find out they have --

22 MS. ROSENTHAL: I don't know what my --

23 MS. CONEY: -- they have a healthy, normal  
24 sensibility about privacy. If you think about that,  
25 that's the way adults view privacy. It's contextual.

1 It's based on relationships. It's based on what's  
2 important in our lives. They see the world in the same  
3 light. The things that they think are important may be  
4 different than the things that adults believe are  
5 important, but they have a healthy sense of privacy that  
6 should be respected.

7 We need to better understand their role and  
8 their relationship with privacy, but not generically  
9 dismiss them as having no interest in privacy.

10 MS. ROSENTHAL: Thanks, Lillie.

11 Anyone else? Oh, Nicole.

12 MS. WONG: I totally agree with that, and we  
13 got homework. The folks on the panel got homework, which  
14 included a great article by Danah Boyd about, as an  
15 educator, how do you deal with kids on social networks,  
16 which I thought was really interesting.

17 And I think what she pointed out was there is  
18 only so much you can do in terms of regulation or trying  
19 to, you know, keep them cabined in a certain area,  
20 because in a lot of cases they know more than their  
21 parents do about how to get around those firewalls or  
22 whatever it is you build.

23 And so the answer is about education and  
24 modeling well and teaching anything -- and here's the  
25 vulnerability I think for kids. It's about judgment,

1 right. Have we taught them to exercise the right level  
2 of judgment about their privacy or who they friend or  
3 don't friend or upload to a particular service.

4 And the answers to those are hard because they  
5 are about better education and better parenting. The one  
6 thing I was just -- my daughters have recently, they have  
7 an annual checkup, and every annual checkup the doctor  
8 will ask them a question like do you know how to cross --  
9 what do you do when you cross the street; what do you do  
10 if a stranger comes up to you.

11 And this year the question was: What do you do  
12 if someone wants to chat with you. And that's the thing  
13 that we have to do for kids, right. Those are the  
14 questions and the type of modeling and parenting that we  
15 have to start at those ages.

16 MS. ROSENTHAL: And is it just the parents?  
17 Should anybody else be on the hook for educating minors?

18 MS. WONG: It takes a village, that kind of  
19 thing, and the FTC probably has some little bit of it. I  
20 do think we all have to get better at it.

21 MR. MAGEE: All right. So we -- I'm sorry,  
22 Erika.

23 MS. ROTTENBERG: Just a real quick comment. I  
24 don't disagree with what's been said, and what I would  
25 say is that for every benefit in the world there are some

1 down sides or there will be abuses. And you know people  
2 pick -- for a future employer to request a user name and  
3 password, I mean people shouldn't be exposing their user  
4 names and passwords.

5 Now if there is information that's posted and  
6 it is available to the public, I would suggest that it's  
7 okay for the world to see that because the user is making  
8 that choice. But you know, am I going to hand the key to  
9 my house to my employer? No. And so it's where are  
10 those boundaries. And, again, there will be abuses and  
11 abuses should be addressed.

12 MS. CONEY: I would add one point and then we  
13 can move on. The dynamic between power and the ability  
14 of persons who are vulnerable to exercise those rights in  
15 a knowledgeable way is also buttressed by laws and  
16 regulations that protect them. And there were -- I mean  
17 we can go on and on about labor abuses and mistreatment  
18 of people.

19 If we didn't have OSHA, if we did not have  
20 labor laws, if we didn't have time management laws or  
21 limitations on how many hours people could be asked to  
22 work, those abuses would still be there. We have got to  
23 be more aggressive in acknowledging the role of  
24 regulators and legislators in protecting people.

25 You can't expect the children or their parents

1 or for the consumer to be able to have the same weight  
2 and voice in the environment where a lot of data  
3 collection is happening.

4 MR. MAGEE: Chris, quickly, and we'll move on.

5 MR. CONLEY: Just a follow-up to Nicole's. I  
6 agree that a lot of the responsibility for children has  
7 to come from their parents. But when we are talking  
8 about technologies that the parents don't understand,  
9 that's not a solution. We have to make sure that the  
10 parents, that teachers, that everyone else is also  
11 educated about the consequences of these choices online  
12 so that they can help their children understand what they  
13 mean.

14 MR. MAGEE: That's a good point. So we have  
15 talked about some of the benefits that we see and some of  
16 the challenges and risks of potential harm, as well.

17 What I'd like to focus on for a little bit is the idea of  
18 unexpected sharing, that seems to be where a lot of the  
19 potential problems come from, and talk about the  
20 dichotomy between the expected and unexpected sharing.

21 When a consumer perhaps puts too much out on  
22 their social-networking page, is that a matter of  
23 misunderstanding how much control they have over who gets  
24 the information? And, if so, how do we approach that?

25 Dennis, you haven't talked. How about it?

1           MR. YU: So a couple of years ago Facebook  
2           opened up a platform where developers could create games  
3           on top of the information that users had, and it wasn't  
4           just Facebook. It was OpenSocial, and it created an  
5           amazing opportunity where you had a friction-free  
6           environment that you could have games where, you know, I  
7           could send a gift to Nicole and she could throw something  
8           back at me, and there was a lot of interaction.

9           But the trouble is that consumers weren't aware  
10          that that information was being shared with an advertiser  
11          and the application developer and a DAT network and  
12          various other affiliates or players in the game. And any  
13          time you have a new means of advertising there are rules  
14          that are going to be maybe just a few months behind to  
15          play catchup, right.

16          There is going to be a few players that are  
17          going to try to come in first to abuse the system that  
18          may try to create a bad version of personalization,  
19          right. Good personalization is, I know who you are. I  
20          know what your preferences are and I'm going to deliver  
21          you something based on what you like to see.

22          So if, for example, on your social-networking  
23          profile I did this, just to see, right, I changed my  
24          preference to, you know, male seeking male, and I saw I  
25          was flooded with a lot of, you know, male seeking male

1 ads. Or I changed my religious preference to say that I  
2 was Jewish, and I saw all these Jewish ads, right.

3 And it's just amazing where it can be good  
4 personalization, but sometimes the data can be used in  
5 ways that are unintended; and social-networking sites, I  
6 think Facebook in particular, has done a great job in  
7 clamping down on when there are these unexpected  
8 situations.

9 But anytime you release more data that's going  
10 to create an opportunity for situations you haven't  
11 thought about, because other people are going to be  
12 playing in the space. And especially, back to what  
13 Lillie and Chris were saying about teenagers, they are  
14 not really aware.

15 They're in general not as concerned about the  
16 sharing. So they don't know, necessarily, that their  
17 data is being shared. Even though there is a little  
18 thing saying do you understand this is a third-party  
19 application and so forth. And, to Nicole's point,  
20 definitely the education to make sure that users are  
21 aware of what's going on with their data, that if they  
22 are playing an app and it says, hey, you need to put in  
23 your cell phone number to be able to get your score, then  
24 they should know better than that.

25 MR. MAGEE: Well, so what are some ideas for





1 I know some of the other services are doing, as well,  
2 that we shouldn't be in a position of making choices for  
3 users.

4 We should give them the information that they  
5 need. We should help them understand what the possible  
6 implications are and then we should get out of the way.

7 I think that's where innovation is important. We can't  
8 be in a position of trying to control people's attitudes,  
9 particularly when we are talking about a free service, a  
10 voluntary service.

11 People don't have to social network. They can  
12 do all sorts of other communications. If you want to  
13 share pictures. There is a myriad of sites on the Web to  
14 do. If you want to communicate with people, you can pick  
15 up the phone. You can send an email. I mean, there are  
16 a whole series of technologies that people can engage in.

17 And I think people forgot that the users are  
18 smart and they do understand what's going on. A good  
19 example. We just recently went through a much ballyhooed  
20 conversion for people where we asked every single one of  
21 our users to stop and think about privacy for the first  
22 time.

23 And there has been a lot written about, boy,  
24 people sure aren't going to understand what's going to  
25 happen, and people are really going to be confused about

1       that. A lot of people speculated and they worried aloud  
2       about it. I did, frankly. I spent a lot of time  
3       thinking about it with the teams that I was working with  
4       within Facebook before this happened.

5                But what happened was something really quite  
6       remarkable. Facebook put in front of our 350 million  
7       active users a moment when we said, please stop and think  
8       about privacy. Here's what's actually happening with  
9       your information. Here's where we think the information  
10      is important to you, and here's the controls that you can  
11      use to exercise as much or as little control as you want  
12      over it.

13             And we found something extraordinary. We had

1 and we are pretty excited about it.

2 MR. MAGEE: Chris.

3 MR. CONLEY: So Director Vladeck pointed out  
4 earlier that one of the most emailed articles in the New  
5 York Times right now is about setting your Facebook  
6 settings. So I think that shows that at least some  
7 people think that there is more information that they are  
8 learning as they go along.

9 They've just seen the choices that Facebook  
10 presented was not enough for them to feel like they had  
11 the answers or that their friends had the answers, that  
12 it's very hard to make -- and acknowledging -- it's very  
13 hard to make an intuitive user interface here.

14 And also I have several comments at the end,  
15 but I'll save some of them till we get to applications.  
16 But what I wanted to talk about is defaults. So when we  
17 are talking about user expectations, some of the question  
18 is about what do you make the default settings.

19 And the reality is you can't have a default  
20 setting that it is everyone. You can talk about what the  
21 user norms are and what people think, but you can't have,  
22 this is a default and say you have not shaped  
23 expectations by it, because some people, that's what they  
24 would choose, and some people, that's what they would  
25 not.



1 at LinkedIn take great pains, as I'm sure, my colleagues  
2 do in terms of what is it that we think most of our users  
3 want. You are absolutely right.

4 One size isn't going to fit all, not for an  
5 individual and not for the same individual over a period  
6 of time. And we want to provide the opportunity in an  
7 easy, understandable manner for folks to say, you know, I  
8 want to provide or share this piece of data with these  
9 people, but not for these people, and it's the ability to  
10 do that.

11 And, again, we won't necessarily get it right  
12 for everyone all the time, but it's with serious  
13 consideration in looking at how our users are using the  
14 site; and, based on user feedback, what do most of our  
15 users want. How is it that we can use the network.

16 And something else. You know I think Tim said  
17 we trust our users to make the right decisions. And I  
18 agree with that, but what I would also say is that our  
19 users trust us. And the marketplace will speak. It  
20 takes a long time for users to trust an ecosystem, and we  
21 have 55 million users.

22 If we were to breach that trust, if we were to  
23 mis-use information, if we were to suddenly sell user  
24 data when we tell people that we don't sell user data, we  
25 can breach that trust in a heartbeat. And our interests

1 are aligned with our users, because if we breach that  
2 trust, our ecosystem will fall apart.

3 MR. MAGEE: And that's a great point. I want  
4 to just -- if we can quickly hear from the other  
5 panelists with their tents up and then we'll move on.

6 Nicole.

7 MS. WONG: So just in terms of the consumer  
8 expectations, I think what you are hearing from Erika and  
9 from Tim is part of the hardest thing that we try to do  
10 is to figure out what the expectation is, because in a  
11 world where the new mediums are changing so quickly,  
12 right, like there is a new startup that will be announced  
13 next week which will completely change the way we  
14 communicate with each other, and then there has got to be  
15 a new norm that develops around it.

16 So theorizing out with that expectation and then  
17 coding a UI to meet it is a really, really difficult  
18 task. One of the things that we did today in honor of  
19 International Day of Privacy Day was we actually just  
20 announced for Google what our privacy principles are, and  
21 we are hoping that that really communicates to the world  
22 the things that we do.

23 When I and my team sit down with our engineers  
24 here the things we go through. The first one is is there  
25 value for this product for our user, because that's

1 always got to be the thing that leads. The second is can  
2 we build in the best possible privacy standards into that  
3 product, whatever that might be, whether it's health or  
4 social or search.

5 The third and fourth are the two key ones that  
6 I usually end up talking a lot with the engineers about,  
7 which is can you build in a transparent UI that really  
8 explains to the users as they use it they don't have to  
9 go read a privacy policy, as they are using it they  
10 intuitively understand what's being collected and how  
11 it's being used.

12 And the fourth is creating real control so that  
13 you build an interface that gives a user really  
14 meaningful and granular controls. In the 2000 era of the  
15 Web, usually your choice was binary, like use or don't  
16 use. If you don't like the privacy policy, this is not

1 secure. I thought it was interesting, Peder, what you  
2 were raising, which is should you give users kind of like  
3 the training wheel period of figuring out the UI before  
4 you like set them free with it.

5 And I think it's a really interesting idea.  
6 Internally as we develop a product we not only use focus  
7 groups of users, but we actually -- we do what we call  
8 dog-fooding, which is we in the company all use a product  
9 before we release it so that we get a better sense for  
10 how users expect a UI to behave or a product to behave.

11 I think the challenge of having the training  
12 wheel phases, when we actually see our users come to us  
13 they are across a spectrum. There are the beginner green  
14 folks and the double black diamond folks, right, and they  
15 are all coming at the same time. So I think that the  
16 challenge of that would be to figure out how do you focus  
17 that UI to the right user.

18 MR. MAGEE: We have got to move on. Dennis, I  
19 know you have got your tent up. I think Michelle's got a  
20 question she's going to direct to you. So maybe we can -  
21 -

22 MS. ROSENTHAL: And this goes to consumer  
23 expectations, but it also moves us into the third-party  
24 application discussion. So do consumers understand when  
25 they are on a social-networking site or a platform that



1 they -- when they are dealing with the social-networking  
2 site or the platform, and when they are dealing with the  
3 third-party app?

4 MR. YU: For the most part, consumers do  
5 understand because social-networking sites have put a  
6 notice saying this is an app that was not built by  
7 Facebook or MySpace, but what they don't understand is  
8 what level of data sharing is there. And just because  
9 you have the terms of service and the privacy policy,  
10 they don't understand that their information,  
11 information's in their profile, information about their  
12 friends is being shared.

13 And so that has caused an opportunity for just  
14 a few people who want to spoil it for the others to come  
15 in and abuse that, and there is certain measures that we  
16 need to think about and how to play this cat-and-mouse  
17 game on protecting that base of users that otherwise  
18 doesn't know any better.

19 I agree with Tim and Nicole that if you trust  
the users, they will be able to figure it out. There are

1           So in the same way you have feedback mechanisms  
2           in an auction site like on eBay, I think you are going to  
3           see more and more of that inside social networks, right,  
4           because the more data you have, the more nuanced you are  
5           in terms of, I'm going to turn this on, I'm going to  
6           expose this to just my friends or this to just coworkers.

7           You are going to see a lot more of that and  
8           users are going to have -- with that kind of control  
9           you'll have less of the current problem, which we like to  
10          call virtual blight, right, which is advertisers that are  
11          going to pretend that they are a brand; hey, I'm  
12          Southwest Airlines, I'd like to give you some free  
13          tickets.

14          Well, how do you know if that's really  
15          Southwest Airlines or not, right? So when there are a  
16          few bad advertisers it can cause other people who are  
17          legitimate advertisers to have a bad experience because  
18          users are going to say, you know what, I've been fooled  
19          by a couple of these ads before; I don't know if that's  
20          really who it is. So it imposes a negative externality  
21          on the other guys.

22          MS. ROSENTHAL: Okay. Lillie, we are going to  
23          get to you in a second, but maybe you can just frame the  
24          third-party app discussion a little bit and talk about  
25          how these third-party apps are monetized and sort of how

1 the businesses are run. We know there is a big  
2 difference between the -- we talked a little bit about  
3 the barriers.

4 There are low barriers to entry, which is great  
5 in some ways, but then you sometimes have a small startup  
6 that's not worried about reputation or things that a  
7 larger company might be worried about. So how do you --  
8 maybe you could talk about those, the dichotomy there and  
9 how these businesses are monetized, and then we can start  
10 talking about -- we can talk more about the third-party  
11 apps.

12 MR. YU: For better or for worse, the  
13 expectation is that social-networking sites are free and  
14 because of that whoever's building an app, they have to  
15 make money off of advertising because they are not going  
16 to charge a monthly subscription.

17 This is not World of Warcraft where you are  
18 charging ten bucks a month. It's a different kind of  
19 user. So whenever you have this new land that opens up  
20 the vultures are going to come in first. And, therefore,  
21 you are going to see a lot of advertising that may be  
22 misleading.

23 And Facebook, MySpace, it's not so much with  
24 LinkedIn, but you are going to see these kinds of ads  
25 that will try to say, you know, give me your cell phone,

1 install this toolbar or sign up for this particular  
2 offer. We have seen a lot of the advertising -- this was  
3 -- not anymore, but this was a couple years ago just when  
4 we were all working together to try to figure out what to  
5 do, a lot of noncommerce related items, right, because  
6 people weren't on a social network site to check out, to  
7 put in their credit card, right.

8 We'd run ads for hey, you know, if you are  
9 sending virtual gifts why not send an actual box of  
10 chocolates for Valentine's Day, and we found that that  
11 was -- that was not effective, because there was the  
12 expectation that things would be free. And so that  
13 created a number of small guys.

14 These right in the beginning there weren't big  
15 companies like Zinga, other guys who want to play by the  
16 rules; you got a lot of teenagers. I remember, there  
17 were some teenagers that were paying 10,- to \$20,000 a  
18 day in earnings off of their advertising.

19 This is some kid in his dorm room. He made  
20 this game just for fun and now he's making 15 grand a day  
21 off of advertising? He's going to keep doing that and  
22 yeah, he'll get shut down, right, because there is policy  
23 enforcement. There is different kinds of -- there is a  
24 whole process to catch that.

25 But then he's going to turn around and he's

1 going to make another app and he's going to make 20 other  
2 apps that are just like that, and all of his friends on  
3 the forums are going to say, wow, you are making how much  
4 money; how do I get in on this, too, right? And that's  
5 normal, right.

6 And I believe Facebook -- I don't want to say  
7 it's all about Facebook -- but there is a normal  
8 progression of putting rules in place to be able to stop  
9 the bad things these guys are doing.

10 MS. ROSENTHAL: Okay. So, Tim, how do you deal  
11 with that?

12 MR. SPARAPANI: We have got a really aggressive  
13 policy about handling applications, and it's difficult  
14 because we have an open platform, which is one of the  
15 advantages of Facebook. You can build an application.  
16 As you said, there is a very low barrier to entry and  
17 people can be off and running and creating new goods and  
18 services, which are by and large tremendously  
19 advantageous to the public.



1 do with data they collect, or whether they ought to be  
2 allowed to collect information on consumers, all of that  
3 information is -- those questions haven't been really  
4 resolved.

5 It's not whether the size of the entity; it's  
6 the activity itself that is a problem. And as far as  
7 consumer control, even in the examples that have been  
8 discussed on the panel with Facebook, the control  
9 message, it's limited. It's not really real control.

10 You have control in a lot of physical things  
11 you do in the world, but in the social-networking  
12 environments the control -- consumer control is being  
13 defined by the companies. When network settings were  
14 changed and it did affect negatively the privacy rights  
15 of users, their control wasn't present or even a part of  
16 that equation.

17 So having a level playing field, defining what  
18 the privacy rights of consumers are, I think that's the  
19 model we should pursue, regardless of the size of the  
20 entity or if they are application developers or not.

21 MS. ROSENTHAL: Okay. We have an audience  
22 question and I think it's a good one. So I'm going to  
23 share -- sure.

24 MR. SPARAPANI: This problem, such as it is, is  
25 relative in scope to the size of the advantages which are

1 created by applications. It's a small problem, as Dennis  
2 I think was making clear. Yet nevertheless this is where  
3 our economy is going. If you ask people in the valley,  
4 this is where the energy is.

5 It is around applications for a myriad of  
6 platforms, some of which are represented up here on the  
7 stage. This is going to require more than the activities  
8 that even a small staffed company like Facebook is. We  
9 actually don't have that many staff. We are going to  
10 need help.

11 We are going to need the FTC to play a serious  
12 role here, to talk to these third-party companies and  
13 take actions when they do things that are not in --  
14 comporting with users' expectations. The FTC, various  
15 local governments, the federal government will have to  
16 play a role, because only in that way can we have open  
17 systems, and yet have the advantage of applications,  
18 while diminishing the likelihood that some applications  
19 will be inappropriately acting.

20 MS. ROSENTHAL: Chris, Tim is talking about  
21 user expectations with respect to the data that third-  
22 party apps are getting and using and what they are doing  
23 with it. But how can users actually complain and step  
24 forward and say, this is a problem, if they are not  
25 necessarily aware of what the practices are? Can you



1 talk a little bit about that?

2 MR. CONLEY: I can talk about that in a lot of  
3 different ways. I think, in fact, just that specific  
4 questions, one of the questions I would have for Tim is,  
5 you know, Tim, Facebook has, LinkedIn has a lot of  
6 platform and social networks have some kind of auditing  
7 and you know, they actually identified that app. And  
8 they send notices and they cease and desist.

9 But how often is it public information about?  
10 How often do you send a warning? How often do you  
11 question or audit? How often do you do this, because  
12 without that kind of information there is no -- the  
13 consumer doesn't have a real idea of what's going on,  
14 what kind of risk is there in using applications, what  
15 percentage of applications.

16 You say it's a small number, but is that 10  
17 percent, one percent, .1 percent, what. And then it also  
18 -- for -- from the policy's perspective without some idea  
19 of how often this is happening, how much effort do we put  
20 into regulating? So very narrowly, that would be my  
21 answer to that. I can talk more about other things, but  
22 --

23 MS. ROSENTHAL: Well, yes. Ian, do you have  
any -- your company obvi5rt do we put 18 h72Sh o yo -2 -2.2678s18 h72Sh iPhTD , lwe put

1 believe, and also on Facebook.

2 MR. COSTELLO: We are on the iPhone and on  
3 Facebook, and I just want to call out that, yes, while  
4 there is a small problem of apps that are not behaving as  
5 they should, there is a large number of apps that are  
6 using this data that they are getting from Facebook and  
7 others as their lifeblood.

8 And that's kind of what drives the engagement  
9 there, and I think as long as and very supportive of  
10 Facebook's developer policies that we are not storing  
11 this PII. We are using it to engage users, not to share  
12 with third-party networks and things of that nature. So,  
13 again, this problem I think is limited in its basis and  
14 most entities out there are actually playing by the  
15 rules.

16 MS. ROSENTHAL: Some have discussed that maybe  
17 these platform providers and social-networking sites can  
18 reduce the amount of data that goes to the third-party  
19 app. Do you think that that -- you seemed to touch on  
20 that a little bit. Do you think that that would affect  
21 the innovation among these applications?

22 MR. COSTELLO: Yes. Again, I kind of  
23 referenced that as the lifeblood. One of the examples we  
24 have, one of our apps is pick your five, where it's  
25 basically pick five things and you can pick five

1 anything, and I can pick five places that I've lived or  
2 my five favorite TV shows or my five favorite movies and  
3 share them with my friends.

4 And one thing that we found is that it's very  
5 valuable to have users then see the popular pick five  
6 that their friends have done in order to then do those --  
7 well, so we kind of use this data that's shared to us and  
8 it's not -- again, when you pick five you hit a button  
9 that says, share with my friends, so it's nothing that's  
10 out of the consumers' expectation. But, again, we use  
11 that data to drive engagement, and I think that limiting  
12 that would also limit the engagement and limit the  
13 innovation, I think.

14 MS. ROSENTHAL: Okay. Thank you.

15 So, Chris, if there are going to be tons of  
16 games and apps and all of these things available on the  
17 Web, you have talked about the privacy by design concept  
18 in the past. Is that -- how do we bake in privacy to  
19 these apps to make sure that when information is  
20 collected that it's used for the purpose that it's  
21 collected for?

22 MR. CONLEY: Well, I'm going to start by  
23 talking a little bit about the application we wrote. So  
24 we look at Facebook and not to pick on Facebook, just  
25 because they were the one we were focused on at the time,

1 and I learned six months ago maybe that how much access  
2 Facebook applications have to information just by  
3 default, if you run an application.

4 It has access to everything. It doesn't matter  
5 whether this is pick five telling me, you know, what are  
6 your five favorite politicians or whether it's which  
7 Disney princess do you most resemble. Applications have  
8 access to everything.

9 In fact, when you run an application on  
10 Facebook right now, if you -- excuse me -- if you haven't  
11 changed your default settings, when your friend runs an  
12 application, that application also has access to most of  
13 your profile information, to your political preferences,  
14 to the groups you have joined, to the pages you are a fan  
15 of, to your friends' lists, to all sorts of information,  
16 and we found that to be surprising.

17 I think of myself as an educated Facebook user,  
18 aware of privacy, and that was something I wasn't aware  
19 of. And we decided one of the tools we would use to help  
20 people understand this is, we would write our own  
21 application, because as I said, you don't have to be a  
22 professional to write an application.

23 You can be, or you can be someone who hasn't  
24 written a program in about seven years and wants to dust  
25 off some skills and see what he can come up with in a

1 couple of days. And so we wrote a little quiz of our own  
2 that's basically is a quiz about how much do you know  
3 about how applications access information.

4 And if you take the quiz, and probably some  
5 have, some haven't, you can find out that if you run a  
6 quiz, whatever the question is, the quiz can still see  
ytiotquesrrrrrrrrrrrrrrrrrdGhl mhr-2.tan still see

1 brought a printout of some of the names of people who  
2 signed a petition asking for more privacy.

3 This print's a little small for the 50,000 plus  
4 people who were on our signature. But going back to the  
5 question, which I think was how do we frame this, one of  
6 the things we asked for is more control over -- more  
7 transparency about what applications see.

8 If you have the five best application, it's  
9 asking for your five best things, why does it need to  
10 have access to my political preferences? Why does it  
11 need to have access to my friends' friends' list? Why  
12 does it need to have access to any of this?

13 Make it very specific what it is the  
14 application needs so that I can make an informed choice  
15 about whether to share that with the application. I  
16 think Tim will probably comment on this, but that's one  
17 of the proposed changes.

18 The other thing, of course, is making sure that  
19 I have control over my own information. Even when my  
20 friend runs an application I should be able to choose  
21 whether or not that application can see my information,  
22 and that's one of the concerns we have right now, is that  
23 there is no longer, as of Facebook's recent changes,  
24 there is no option to opt out of my friends share  
25 information with applications entirely. That was an

1 option; now it's not.

2 Applications can always get information about  
3 my friends' lists and my connection and things like that.  
4 And we would like there to be more control so that I can  
5 make informed decisions about whether or not I share each  
6 and every bit of information.

7 And, again, going back to defaults, the  
8 defaults for most of this are, applications can see  
9 everything, and I would prefer to rethink that and say,  
10 well, maybe we want to have people choose whether or not  
11 they want to participate in the application ecosystem, as  
12 opposed to just the social-networking ecosystem before  
13 their information is available to everything.

14 MR. MAGEE: Okay. I'd like to switch gears a  
15 little bit and talk about what incentives there are for  
16 protecting privacy in this space.

17 And I was struck by something, Erika, that you  
18 said, that LinkedIn would be very concerned about the  
19 possibility of losing their consumers' trust.

20 And I'm wondering to what extent social-  
21 networking sites, other platforms, are competing on  
22 privacy and whether there is a realistic chance that,  
23 say, a consumer who's devoted a fair amount of time and  
24 energy into creating a profile and creating a list of  
25 contacts would simply pick up and move to another,

1 similar site that perhaps has a little bit of -- a better  
2 privacy practice than the former.

3 MS. ROTTENBERG: So I believe, and I think that  
4 LinkedIn believes, that while we don't necessarily  
5 overtly compete on privacy, again, if we were to breach  
6 the trust that the users have placed in us, and truly  
7 breached the trust -- the trust that the users have  
8 placed in us, people would pick up and go elsewhere.

9 MySpace, for instance, you know, is one of the  
10 first networking sites around, and not that they breached  
11 users' trust, but there have been individuals or users  
12 who have decided to move to another platform. It is a  
13 free platform. People can -- users can wake up today and  
14 say, you know what, I'm done with LinkedIn or I'm done  
15 with Facebook or I'm done with choose your platform, your  
16 networking service, and I want to close my account and  
17 we'll close that account.

18 Users could say, I want to, you know, delete my  
data and we will delete data. I mesT.(12 )8415 0 TD (15 )Tj 2-ep.on8ue'732 b oon8ue3e1uSTj 2.8415I wac



1 users," and trust is in the DNA of our company with  
2 respect to each product release or feature release that  
3 we put out there.

4 MR. MAGEE: Nicole.

5 MS. WONG: I'll just be really clear. We  
6 compete on privacy. We do that in terms of trying to  
7 develop the best possible products that are privacy  
8 sensitive. We do that because we have an entire team of  
9 engineers specifically dedicated to privacy, and a cross-  
10 functional group that meets every week that involves  
11 everyone from engineers to policy people to legal people  
12 to talk about the biggest issues in privacy.

13 We absolutely compete in this space. One of  
14 the things that happened last year which I was so  
15 thrilled to see because it was an engineering-driven  
16 idea, and in our company the engineering-driven ideas are  
17 always ones that work out best, was a group of engineers  
18 who named themselves the Data Liberation Front.

19 And what they did is they basically took a page  
20 from what we had done when we launched Gmail in 2004.

18 20 whj2.8eb t( -2. we Aaoma4.)Tj -2.8415 0 TD (2ss, When Gmaan speengineers do 2ssata Liberation Front23)Tj -2

1 move all your emails. You do not have to shuffle them  
2 over one by one; all of them easily to the next service  
3 if you decide you don't like us. Well, our engineers  
4 last year decided we should do that for every service.

5 And so they have had a concentrated effort over  
6 the last several months to take every one of our services  
7 where a user creates and stores their data and let them  
8 make it -- move it to a different service or download it  
9 to their own computer if they want.

10 They've now hit 25 different services. Every  
11 one of those services has a feature for portability, and  
12 what I love about that is two things. The first and most  
13 important one, I think, is that what we are trying to do  
14 is get users to engage with their own information.

15 So when you build in that portability what you  
16 are signaling to the user is: This is yours and you can  
17 take responsibility for it and understand whether you  
18 want to stay with us or go. But that level of engagement  
19 and exercising the muscle of control is something we  
20 actually have to start to get users to do, because they  
21 have been living in a world of sort of passive Web  
22 absorption and that sort of thing for a while.

23 And most times users, when they come to a new  
24 service, don't think about how am I going to end this  
25 relationship if I don't like it in three months or a

1 year? What are my options at that point? What our  
2 engineer said is, you should be able to end that  
3 relationship. You should be able to move your data, move  
4 it freely, like as in it won't cost you any money and it  
5 shouldn't take you a lot of time. And that was one of  
6 our priorities.

7 The second thing I love about that is that it  
8 forces us to be better, and this is a little bit towards  
9 what Erika was saying about trust, that because our users  
10 literally can go to a competitor with just a click, it  
11 means that we have to be better with every product, every  
12 day, because they can leave, and that makes us develop  
13 better products.

14 MR. MAGEE: I think that's very interesting,  
15 this idea of the portability, but doesn't it also raise  
16 some privacy concerns? For instance, if a user picks up  
17 and moves from one social-networking site and is able to  
18 take all their contacts and the information about those  
19 contacts to a different social-networking site, are those  
20 contacts that have been transported over to a new  
21 platform, do they have any say in the matter? Perhaps  
22 they don't want to be associated with the second  
23 platform. It may have a different angle or a different  
24 slant?

25 MS. WONG: Yes. So the contacts lists I think

1 are different and I'd have to go back and look at the  
2 specific feature for contact lists. The emails, right,  
3 it's literally, like, take all the email content that you  
4 have and put them in a different container and the  
5 features that we are talking about are typically like the  
6 documents, the calendar, in which case these are, you  
7 know, it's like your home calendar now, right?

8 You have names of people that you are going to  
9 go see, your doctor's appointment or dentist appointment.  
10 You don't give your doctor the option to be taken out  
11 when you switch calendars. That's just what goes along.

12 MR. MAGEE: Tim, did you want to weigh in? You  
13 had your tent up for a moment.

14 MR. SPARAPANI: I was just going to associate  
15 myself with the comments both by Erika and Nicole. We  
16 absolutely intend to and do compete on privacy. There  
17 are virtually no barriers to entry, to creating a new  
18 social network. You can do it quickly. Lots of people  
19 do. They're numerous.

20 There are dozens of competitors around the  
21 world that we have, and there will be more, I am sure.  
22 So we intend to distinguish ourselves through privacy,  
23 and I think you have seen that our model has been one to  
24 look at the fact that there are not harmonized laws  
25 between the U.S., Canada, Australia, and Europe, and we

1 have tried to say, given the impasse, we are going to do  
2 something different.

3 We are going to do privacy by design. We are  
4 going to give people new tools. We are going to innovate  
5 in the space and that's how we are going to distinguish  
6 ourselves and that's how we are going to grow our user  
7 base. And, in fact, I think our users have learned to  
8 trust us and they do continue to trust us. And so we  
9 absolutely compete on privacy and that's all I wanted to  
10 add.

11 MR. MAGEE: So it sounds like one of the  
12 incentives for competing on privacy is this concept of  
13 user trust. But is there a tension here between -- Tim,  
14 you have mentioned a few times that Facebook's a free  
15 service -- but I assume at some -- you are monetizing in  
16 some way.

17 Is there a tension between protecting  
18 consumers' privacy and monetizing from the perspective of  
19 a platform of a third-party application?

20 MR. SPARAPANI: I think it would be impossible  
21 to say no. I mean, of course there is a tension. But I  
22 think you will see throughout Facebook's history we have  
23 -- and I'm very proud of this -- we have chosen again and  
24 again and again a really fantastic user experience over  
25 giving a profit-maximizing opportunity.

1           We could spam the heck out of people with ads.  
2           They could get hit with an ad every time they walk in.  
3           They could have huge ads. They could -- ads could follow  
4           them around. We don't do that. More importantly, we are  
5           a walled garden in the sense that we never, ever, never  
6           sell data to third parties.

7           So the data that our users give us voluntarily,  
8           they give it to us in trust and we treat it in trust, and  
9           it is not ours to give to other people. So we run ads to  
10          them. We think that they are useful to them. We think  
11          they enhance their lives. We think they give them  
12          opportunities that they would not otherwise have the  
13          chance to avail themselves of.

14          But we never share their data with anyone else.  
15          So we have made really key decisions which we think our  
16          users have respected and we think they like.

17          MS. ROSENTHAL: Then it -- so Facebook doesn't  
18          give the data to advertisers, but are there ways in which  
19          that data is going to advertisers anyway?

20          MR. YU: That has been possible before where  
21          because of the nature of the game that you are creating,  
22          the application, the application does need that data to  
23          be able to have that interaction. And there are a few  
24          bad apples, and there is just a few of them that will  
25          actually sell, and it's completely against the terms of

1 service and it has been an issue before.

2 But I've seen where Facebook has taken action  
3 to try to shut these other people down, but that's always  
4 going to be the case anytime you have a developer with  
5 access to data, right, because you had a free service.  
6 Other people who may be thinking otherwise, they are not  
7 a large brand, they are going to think, well, can I make  
8 money here or do I want to do what's right in the long  
9 run for users.

10 MS. ROSENTHAL: Do you have any audience  
11 questions?

12 MR. MAGEE: Yes. We have a couple of audience  
13 questions. I'm going to paraphrase, but there seems to  
14 be some question about, "Although many social-networking  
15 sites allow users to delete data, in many cases the data  
16 is not deleted at all, but rather, it's hidden from  
17 view."

18 And there is another one about, "What does it  
19 mean to delete or liberate data?" Perhaps somebody could  
20 weigh in on that?

21 MS. WONG: Well, for us, I mentioned the data  
22 liberation -- liberating means portability, the ability  
23 to take the information that you have created and stored  
24 on our system and move it to someplace else.

25 MR. SPARAPANI: If you tell us that you want --

1 or I'm sorry. Let me back up. If you tell us that you  
2 want your data deleted, it's gone. And I can't tell you  
3 how many times a week we get people who said, I really  
4 didn't mean to delete it; what I meant was to deactivate  
5 and can I have it back, and the answer's no. It not  
6 there anymore. It's gone. And so --

7 MR. MAGEE: It's not there on the platform.  
8 But of course, if someone has disseminated this  
9 information and it's been passed on down the line it  
10 could still be somewhere?

11 MR. SPARAPANI: There could be bits and pieces  
12 that might be out there existing on other people's  
13 profiles or on their pages, but the actual user created,  
14 generated data en masse is gone, and it's gone for good.

15 MR. MAGEE: Chris.

MR. CONLEY: There is ut oPtocdvi3 BT /F1



1 are there efforts made to delete all the other records  
2 that identify this person was a Facebook user, or  
3 Niceface user or LinkedIn user or whatever the case may  
4 be.

5 MS. CONEY: Further, on the issue of true  
6 portability, especially when you are talking about  
7 applications like Gmail that gave a huge amount of memory  
8 to users who came online, or the variety and types of  
9 information that may be a part of Facebook page, so that  
10 in effect you might be in a walled garden.

11 Although you can leave, there is no where you -  
12 - there is no other place in the universe you can  
13 actually go and experience that life or the applications  
14 that you have. So that's one issue. Even if you say  
15 people can download this to their desktop or their  
16 personal computing device, that may not really be a  
choice11 3drBamNutdevaemC Allm.84w pore 1lr273 enoat may not really be a

1 But there has been a lot of discussion about real world  
2 relationships and how that may or may not differ from  
3 online or social-networking relationships.

4 So I share -- in the real world I share  
5 information with my parents that I might not share with  
6 my neighbor. I share information with my best friend  
7 that I might not share with my employer. Nothing  
8 personal, guys. So the question is, how do I -- in my  
9 social-networking world should I be given the opportunity  
10 of a user to make -- should there be a differentiation?

11 Should I have the ability to show certain  
12 things to some people that I don't show to others, and is  
13 that available now on social-networking sites? Do the  
14 user controls reflect the real world's complexities?

15 Anyone? Tim -- or Erika.

16 MR. SPARAPANI: No, please.

17 MS. ROTTENBERG: We endeavor for it to reflect  
18 the real world. We look at, how do our users want to  
19 engage with our site. I think that any entity that's  
20 building a site for users is looking at, how can we  
21 reduce friction and how can we mirror or how can we  
22 satisfy the needs and the desires of the user base to  
23 engage with the site.

24 Might you want more granular control in a  
25 particular situation? Sure. You may want to do that.

1 Is it something in the -- I actually think that Nicole  
2 mentioned it. Some of these tasks are very, very hard to  
3 design and to implement. I mean, I've sat through  
4 several meetings in the last week about, how can we  
5 provide additional granular control.

6 How can we, say, okay, I want to set up, not  
7 necessarily different groups, but on a linked in  
8 situation different categories of individuals. It's not  
9 an overnight switch, but I would say yes. I mean, it's  
10 something that we spend a tremendous amount of time  
11 looking at.

12 We continually try to innovate and to develop  
13 and to release product and to satisfy -- the users are  
14 really telling us how it is they want to engage on the  
15 site, and it's something that we spend a lot of time  
16 working on.

17 MS. ROSENTHAL: Thanks.

18 Chris.

19 MR. CONLEY: Here again is that in the real  
20 world your controls are usually when you take an action,  
21 and that's, you know, that's it. That's where it is.  
22 Whereas, on social networks and social media those  
23 controls can be changed later. Something that was  
24 relatively spottily disseminated by you originally could  
25 become public later.

1           We have a sad story that I have to relate,  
2           because that's partly my job, about a student who called  
3           us. And that student is gay. He's from a small town, is  
4           not out to the people in their town, but they were a  
5           member of that on campus group that supported LGBT  
6           students and they were a fan of that group's page on  
7           Facebook.

8           One of the changes of the recent Facebook  
9           privacy transition was to make fan pages public. So if  
10          you go to someone's profile you can see exactly which  
11          pages they are a fan of. That's not information that  
12          that person intended to share when they made the  
13          decision.

14          And when they go back and even with really  
15          clear transition tools it's hard to think about all of  
16          the decisions you have made in the past and how you are  
17          reversing them with a decision in the present. It's  
18          really difficult to fully understand the consequences to  
19          privacy of making a whole category of things more public  
20          than it used to be.

21          MS. ROSENTHAL: Tim, do you want to respond?

22          MR. SPARAPANI: Yes, I need to respond to  
23          Chris' comments, because it's just actually not accurate  
24          what Chris said, and I'm forced to respond. It's always  
25          been the case on Facebook that if you were a fan of a

1 particular organization or cause, you know, believe me, I  
2 used to be at the ACLU and people would consider that  
3 sensitive and damning in some places.

4 I'm actually quite proud of it, but it's always  
5 been the case that if you were a fan of a particular  
6 organization anyone could go to that fan site and they  
7 would be able to find your name eventually. So we did  
8 not in fact make that change. And although the press has  
9 reported to the contrary, I'm here to tell you it's not  
10 true.

11 I did want to respond really briefly to the  
12 question. We have made two really exciting privacy  
13 innovations in this space in order to give people what we  
14 think of as really, truly granular control. And I agree  
15 with Nicole and Erika, this is very difficult stuff to do  
16 in terms of coding.

17 So one thing we did is we gave people the  
18 ability to create circles of friends or family so that  
19 they could choose generally, if I want to do this kind of  
20 sharing I will share with this group of people and only  
21 with this group of people. The second thing that we did  
22 is that we -- over the last several months we gave people  
23 actual control at the moment they are about to share any  
24 piece of data, any piece of data, real publisher control  
25 over that piece of data to decide exactly before they

1 share who they are going to share with, when and how.

2 And that's extraordinary and that's an example  
3 of an innovation in the privacy space that no one had  
4 done before. And we are actually -- our engineers are  
5 really thrilled that we have brought it to the  
6 marketplace. We hope other people will emulate it,  
7 because it truly does give extraordinary granular control  
8 for the first time ever really in the digital age. And I  
9 think we are pretty excited about it.

10 MR. CONLEY: Ten seconds.

11 MS. ROSENTHAL: Yes. Yes.

12 MR. CONLEY: First of all, I do want to  
13 apologize. Tim is correct. It was public in the sense  
14 that if you went to a group's -- or a fan page you could  
15 see the list of members. What has changed is that if you  
16 go to someone's profile you can automatically see the  
17 list of pages they are a fan of.

18 So while the technical publicly available  
19 information is still publicly available, the practical  
20 effects seem pretty significant. And I also do want to  
21 say that it's absolutely true that Facebook has done  
22 wonderful things with making what you publish now much  
23 more granular and giving you more and better controls. I  
24 don't want to entirely just pick on Facebook, so.

25 MS. ROSENTHAL: Erika.

1 MS. ROTTENBERG: And I want to encourage  
2 everyone in the audience and beyond -- and I have always  
3 maintained this -- it again goes back to education, which  
4 is people should look at their settings.

5 And Michelle, yes, you can control who has your  
6 information.

7 I just want to provide a couple of situations.  
8 You know you can decide how you want to be contacted. I  
9 mean I get whatever mail in my snail mail box, and I get  
10 lots of things that I probably get three percent of the  
11 mail I receive at home, not in email, but in the physical  
12 space as mail that I actually want to -- actually, it's  
13 probably less than three percent -- mail that I actually  
14 want to look at or need to look at.

15 On LinkedIn you can control who contacts you.  
16 You can say, I'm willing to be contacted by anyone. I'm  
17 willing to be contacted by people who are within my  
18 network. I'm only willing to be contacted by someone who  
19 I'm connected to. You can decide if you are going to put  
20 an update status on there.

21 Who do you want that to go to? And you can  
22 decide that on a granular basis. We recently announced a  
23 Twitter integration, and you can choose if you want to  
24 have a network update be tweeted out to all of your  
25 Twitter connections at the moment that you are doing it,

1 or you can choose no, I don't want that to go out.

2 Same thing with profile updates. So in many  
3 ways you may actually have greater control in an online  
4 space, if you are educated, than in a private space.

5 MR. MAGEE: All right. That's I think a good  
6 segue to -- we are going to have to wrap up in the next  
7 couple of minutes, but we have heard about a lot of  
8 benefits, some risks and challenges in the space. And  
9 Erika was just talking about some different tools, but  
10 also the need for education, informing consumers how to  
11 use them and what it means for their data to be in this  
12 environment.

13 So my question is: Is the market working here  
14 or do we need some type of government intervention to  
15 establish norms in this space?

16 This is an open question. Lillie.

17 MS. CONEY: I'd be happy --

18 MR. MAGEE: I thought you might weigh in.

19 MS. CONEY: -- I'd be happy to speak on this  
20 issue. EPIC has submitted a lot of, I guess we could  
21 call them love letters, to see about --

22 MS. ROSENTHAL: And we appreciate that.

23 MS. CONEY: And I know you do. You know it's  
24 with deep felt, heartfelt commitment that we send in  
25 complaints and draw the agency's attention literally in



- 1 the best, effective way we know how to identify issues
- 2 where consumers are being harmed. This agency is the
- 3 agency. It's the backstop for helping consumers.
- 4 We like the ecological approach that when there

1 regulation could help is to encourage more transparency  
2 around how often is information disclosed to third  
3 parties through search warrants, or court orders, or  
4 whatever it might be.

5 How often do application audits happen, and how  
6 many applications are banned? You know, this is  
7 information that could be relevant if you want to compete  
8 on privacy, open up a market for privacy. You can't have  
9 a real market without real information.

10 And if that's not coming, if the market itself

1 know. There are a lot of ways that -- there are  
2 crowd-sourcing ways to fix these issues.

3 And I think that education is what's going to  
4 be able to help people understand, okay, someone's  
5 sending me this message, or back to what Nicole's saying,  
6 what do you say when strangers try to chat with you.

7 But I think that's really the solution, as  
8 opposed to limiting the kind of data. If you limit how  
9 much data can be there, then you have cut off a lot of  
10 relationships. You cut off -- for example, in small  
11 businesses we see that these guys are creating profiles.  
12 They're doing business online. It's for the little guy,  
13 right? You are trying to reduce the amount of friction.  
14 If you just come in heavy-handedly, I think it's like  
15 trying to fix a broken washer with a sledgehammer.

16 MR. MAGEE: Okay. Nobody wants that.

17 Nicole.

18 MS. WONG: So you already know my position on,  
19 like, let's educate the market. Let me give you one more  
20 thing, and I can't even take credit for it, because I'm  
21 going to echo something that was said at the last  
22 roundtable you held, because Leslie Harris at CDT is very  
23 smart.

24 You have here some of the best players who have  
25 told you we compete on privacy. But as a regulatory

- 1 agency you have the ability to go and find some of those
- 2 other players who are not as transparent who are not

1 there needs to be significant fact-gathering.

2 I think that having privacy policies that are  
3 clear, intelligible, providing users a choice is key. I  
4 think it's education of companies. You are right, and I  
5 think, Dennis, you talked about small kids -- or college  
6 kids who are in their dorm developing applications and  
7 someone says, you need a privacy policy so they just go  
8 grab it from someplace else.

9 We need to be educating -- I mean people want  
10 to do the right thing by and large, and it's up to us to  
11 ensure that that happens. And I do believe that there is  
12 -- there is self-regulation that's going on and there is  
13 some marketplace, I guess, policing, if you will, that's  
14 going on.

15 MR. MAGEE: All right. Well, I want to thank  
16 all our panelists for a great discussion. We really  
17 appreciate your participation. Thank you.

18 (Applause.)

19 MS. ROSENTHAL: A quick announcement, quick  
20 announcement. This is obviously your lunch break. If  
21 you would like a list of restaurants in the area, there  
22 is one outside on the tables that you walked by when you

Applause.)

1 1:30 p.m.)

2 ASSISTANT DIRECTOR OLSEN: All right. Why

3 don't we get started?

4 We're very pleased to have Danny Weitzner join

11 us. Danny serves as the Associate Admin EAdmisocigor for 2.2404 0 TD (4 )Tj5h -2.I TD (4 ).R2404 0 TD (

12 Direcisocigorthe Electronic FrontieocFoundmiion. We're

13 igotunate to have him here today and look igoward to his

14 remarks.

15 (Applause.)

16

17

18

19

20

21

22

23

24

25

## 1                   REMARKS

2                   ASSOCIATE ADMINISTRATOR WEITZNER: Thanks very  
3 much, Chris.

4                   And I really want to extend my thanks to the  
5 entire Commission for the honor of participating in this  
6 effort. I have to say, just in my own personal opinion,  
7 the FTC is really my favorite agency of the federal  
8 government. I guess I should exclude my own agency. But  
9 you are. And I think those of you who have been around  
10 these issues for long enough know that the FTC really  
11 from the very beginning of the internet era has had a  
12 really critical leadership role in shaping a whole  
13 variety of policy responses to the internet. And I think  
14 the country is better for it and the world is better for  
15 it because, as all of you know, the steps that we take in  
16 the U.S. are watched pretty closely elsewhere.

17                  I gather that the FTC did some things before  
18 the internet too, but that is kind of before my time.  
19 But really I think that particularly the effort that you  
20 all have started now, the team that Chairman Leibowitz  
21 and Director Vladeck have assembled here I think really  
22 bodes well for a serious, thoughtful and effective look  
23 at privacy protection going forward, both in the U.S. and  
24 around the world.

25                  So as a member of the Obama Administration I'm

1 really pleased to have the Commission as a partner in our  
2 efforts. I think since I'm far enough from Washington  
3 that I can say as a citizen I'm happy that you are out  
4 there protecting me individually.

5 I want to talk about the work that we're doing  
6 at the Commerce Department to address privacy questions.  
7 The frame that we chose to take in looking at privacy is  
8 to try to understand the nexus between privacy and  
9 innovation. And I want to talk a little bit about how  
10 we're approaching this initiative, just by giving you  
11 some of our starting premises.

12 The first premise that we start with is that we  
13 think that innovation on the Internet has really depended  
14 critically on the innovative use of information, in  
15 general, and the innovative use of personal information,  
16 in particular. As the internet economy has grown I think  
17 that we can all see that regulatory flexibility has been  
18 critical.

19 There was a careful look led by the Commission  
20 in the mid-'90s when the internet began to become  
21 popular. And I think a very careful, measured approach  
22 to the issues within the purview of the Commission really  
23 helped to get this economy going in a very robust way and  
24 created an environment in which there's a considerable  
25 amount of consumer trust.



1           I think that what we've seen over time is the  
2 careful development of rules that respond to real  
3 circumstances, very careful efforts from the Commission  
4 to target enforcement resources where they matter and can  
5 have an impact. And over time I think we can all see  
6 what's built up is a body of accepted rules and best  
7 practices. Some of those come from the private sector  
8 side, some of those come from the Commission; and I think  
9 it's been a very constructive process going forward.

10           We're at an interesting point, though, where I  
11 think that -- I'll talk about more the sense in which the  
12 internet has really become obviously an essential part of  
13 our society. And so many of the services that started in  
14 the early '90s, many of the social practices that started  
15 in the mid-'90s, I should say, have become kind of  
16 foundations in our lives. And we've got a set of rules  
17 that I think are kind of solidifying around those  
18 practices.

19           But we shouldn't, at this moment, think that we  
20 somehow understand the whole environment, that the  
21 innovation is slowing down or stopping, or that we would  
22 want that to happen. I think that we have a whole new  
23 array of innovative new services, whether they're mobile  
24 services, location-based services, services that take  
25 advantage of tremendously-increased powers of data

1 aggregation and data integration that the Web makes  
2 possible. So we have a whole -- a continued stream of  
3 innovation.

4 And at the Commerce Department, as we start to  
5 look at this, what we see is that certainty and stability  
6 in these environments, along with some flexibility, is  
7 sort of the critical balance that we're trying to strike.  
8 Clearly individuals, when it comes to privacy, need a  
9 sense of predictability and certainty in order to feel  
10 comfortable participating in these new services. And,  
11 just as importantly, innovative new companies need to  
12 have an easy understanding of the rules and the  
13 expectations that they're expected to comply with.

14 I think that what's tremendously exciting for  
15 us is that we're really at the point of a kind of a  
16 converging global rethinking of privacy in both the  
17 online and offline environments. The FTC process is is  
18 obviously an important sign of that. As you know in  
19 Europe, in the OECD context, in Asia, we have multiple  
20 rethink efforts going on. And in many ways the impetus  
21 for our privacy and innovation effort at the Department  
22 of Commerce is that we want to, working together with the  
23 Commission, be able to prepare the U.S. to take a  
24 leadership role in that rethinking process. And I'll  
25 talk a little bit about how we're going to do that.

1           But I want to just stress, it was a question  
2           that Jessica Rich posed last night that really is  
3           animating us in many ways, the question is: Can we have  
4           innovation and privacy protection at the same time? Now  
5           I'm an optimist. I think that we can and we should. I  
6           think that getting that right is going to require a lot  
7           of care. It's going to require a lot of handholding  
8           across boundaries.

9           I think that essential to it is the partnership  
10          that we're creating between the Commerce Department and  
11          the Federal Trade Commission so that we can hopefully cut  
12          through some of the more difficult issues and make  
13          progress. And the obvious question is -- which I'm not  
14          really going to answer -- the obvious question is: What  
15          is that balance? The only way that I know how to begin  
16          to answer that question is, to a certain extent, start  
17          with history.

18          As I said, I only know the history of policy  
19          starting with the internet. Before that, I don't know  
20          anything. But I think that just the history of internet  
21          policymaking is very instructive for us.

22          And I think that in a certain sense in the year  
23          2010 we're entering what you could think of as the third  
24          phase or the third decade of internet policymaking. The  
25          first phase was really exciting. A number of people in

1       this room were around for that. And the internet was  
2       this cool new thing. It was transitioning from a kind of  
3       a plaything in the research and education environment.  
4       It was happening out in the proverbial garages here in  
5       this part of the country.

6               And the attitude, the policy attitude that the  
7       United States took to the internet was a very simple kind  
8       of hands-off, more-is-better, let-it-all-happen, a  
9       deregulatory approach. And by all accounts that worked  
10      pretty well. We had a period of extraordinary growth.

1 have 70 percent of U.S. households, just about, are on  
2 the internet. So it's become clearly an essential  
3 resource for our country, for the world. But, as I said,  
4 I think there are real tensions that are developing,  
5 tensions in the privacy-policy arena, tensions in other  
6 arenas as well. The online-copyright-enforcement arena  
7 and cyber-security arena.

8 And I see the challenge of the third decade of  
9 internet policymaking, what some of my colleagues are  
10 calling internet policy 3.0 -- I'm always leery of  
11 numbering things like that -- but in this third decade of  
12 internet policymaking, the challenge is to get together a  
13 set of policies that provide the certainty and stability  
14 that we need for what has become an absolutely central  
15 and pivotal infrastructure, a set of infrastructures for  
16 our society, but at the same times allow continued  
17 flexibility.

18 I think it's going to mean that we have to take  
19 rules, self-regulatory rules, and statutes and  
20 regulations as well much more seriously. I think we're  
21 going to have to look at in the privacy area questions  
22 such as does the patchwork of rules that we have  
23 governing information privacy do the job at this point?  
24 We have a domestic patchwork, we have a global patchwork.  
25 Does this encourage innovation or does this impede

1 innovation?

2 How can we help move forward so that we have,  
3 as I said, that sense of certainty and stability with  
4 continued flexibility?

5 Does the growing consumer unease about tracking  
6 and profiling and increasingly-intensive data collection  
7 practices, does it help this environment or does it hurt  
8 this environment? How do we address that sense of  
9 uncertainty? Where is the right balance?

10 We're very excited to see the discussion that  
11 the FTC has started. We think that there are some  
12 critical questions that are being asked in today's  
13 workshop that were asked in previous workshops. I think  
14 that, first of all, taking a hard look at the viability  
15 of the current-notice and choice framework is a critical,  
16 critical starting point. And I think the fact that the  
17 Commission was prepared to -- or least some Commission  
18 staff -- were prepared to put that on the table was a  
19 very important step to help us all cut to the chase, as  
20 it were, and really, really face the hard questions here.

21 I think that questions that we see raised on  
22 panels earlier today, questions that are floating around  
23 in the private sector and in academic discussions about  
24 enhanced roles for governing usage of data as opposed to  
25 or in addition to rules governing collection of data I

1 think are very promising directions that deserve to be  
2 explored.

3 I think looking hard at the declining  
4 feasibility of deidentification, the fact that we live  
5 necessarily because of statistical phenomena in  
6 increasingly transparent environments online is essential  
7 to come face to face with. I think hiding from that, as  
8 we've sometimes done in the past, really serves no one.

9 I think it's a very important development that  
10 we see a number of global corporations that do business  
11 in the U.S. and around the world are working to explore  
12 what enhanced concepts of accountability mean. The  
13 critical question there, aside from the process  
14 questions, is obviously the question of accountable to  
15 what, accountable to which rules and accountable  
16 ultimately to whom? But I think this nexus of usage  
17 rules and accountability is a very important direction to  
18 explore and we'll certainly be doing that at the  
19 Department of Commerce.

20 So just let me say a little bit about our  
21 process going forward. I suppose my main message here is  
22 to say that we really want to hear from all of you. We  
23 are just at the beginning of a broad consultation process  
24 that will include commercial entities, civil society, and  
25 academics. We'll most likely torment you with a notice

1 of inquiry that we hope you'll all respond to in careful  
2 detail.

3 And our goal, coming out of this process,  
4 really is to be prepared to shape an administration  
5 policy and strategy on addressing privacy issues going  
6 forward.

7 As I said, the many different parts of the  
8 world are in the process of rethinking the directions on  
9 privacy protection. I think it's important that the U.S.  
10 has a progressive approach and a leading approach in that  
11 process. I think that the process that the FTC has  
12 started is going to be an absolutely critical part of  
13 motivating the dialogue. And we very much look forward  
14 to the partnership with the Commission and with others  
15 going forward.

16 So I think I ended right on time. I failed to  
17 answer Jessica's question, but I promise that we are  
18 working on it. So thanks very much and I look forward to  
19 the rest of the Panel.

20 (Applause.)

21

22

23

24

25



1 PANEL 3: PRIVACY IMPLICATIONS OF CLOUD COMPUTING

2 MS. RATTE: So this is the Cloud Computing  
3 Panel. My name is Katie Ratte and my Comoderator is  
4 Laura Berger.

5 We have a very broad topic to discuss this  
6 afternoon. The term cloud computing captures a vast  
7 range of business models. A common theme is accessing  
8 software, data storage, or other products and services  
9 over the internet. And I understand that that definition  
10 doesn't do much to narrow down what we're talking about.  
11 So I'll try to put some parameters around this particular  
12 panel discussion, so we can try to have a focused  
13 conversation about some of the consumer issues that are  
14 raised here.

15 In the previous panel we talked about one  
16 flavor of what I'll call the consumer cloud. And that's  
17 where a consumer is directly putting their information,  
18 placing their information with a cloud computing Service.  
19 We talked about some of those issues in the previous  
20 panel. And so in this panel we'd like to explore some of  
21 the consumer-privacy issues raised by business or  
22 enterprise uses of cloud computing. That is, the  
23 situation where a consumer gives information to a  
24 business with whom they are interacting directly and then  
25 that business stores or processes the data with a cloud

1 provider.

2 We'll examine some of the consumer-privacy  
3 issues raised there because, as David Vladeck pointed out  
4 this morning, the cost of storing ever-increasing amounts  
5 of consumer data just keep getting lower and lower. So  
6 we want to talk about things like data minimization, data  
7 retention, transparency issues, secondary uses, and  
8 consumer-access rates. We also plan to examine some of  
9 the consumer-privacy issues posed by the cross-border  
10 data flows that are facilitated by this business model.

11 I wanted to spend just a couple of minutes  
12 talking about some things will not go focus on in this  
13 panel. One is data security. Although data security is  
14 a hugely important issue in this area, it's actually been  
15 getting a lot of -- it's been the topic of a lot of  
16 public conversation. So we're really trying to shine a  
17 light on some of the privacy issues that are implicated  
18 by this business model.

19 We also will not be talking about government  
20 access to data stored in the cloud. Again, this is a  
21 huge issue and it's been raised in written comments. But  
22 it's sort of outside the scope of what we can accomplish  
23 in the next hour and 15 minutes.

24 So the groundrules for this Panel are the same  
25 as for previous panels. Panelists, if you have a

1 comment, please raise your table tent on its side. We  
2 hope to keep this very lively. And this is not a shy  
3 group, so I have no concerns that people will chime in as  
4 much as possible.

5 For audience members who have questions, we  
6 have comment cards, so you can write your question on the  
7 comment card. It will be brought up. And for those of  
8 you following on the Webcast you can email your questions  
9 to [PrivacyRoundtable@FTC.gov](mailto:PrivacyRoundtable@FTC.gov)

10 So now I'd like to introduce our very  
11 distinguished panel. To my immediate left:

12 Lindsey Finch from [Salesforce.com](http://Salesforce.com);

13 Beth Givens from Privacy Rights Clearinghouse;

14 Nichole Ozer from the ACLU of Northern  
15 California;

16 Harriet Pearson from IBM.;

17 Paul Schwartz from U.C. Berkeley; and

18 Scott Shipman from eBay.

19 And there are more details on all the panelists  
20 in your packets.

21 So, to start off, I'd like to start with the  
22 discussion of what's new about this model. Because  
23 really we are talking about a form of outsourcing here.  
24 So let's talk a little bit about how this particular  
25 business model is different from other types of outsource

1 services that have been happening for years. And I like  
2 to start with Harriet.

3 MS. PEARSON: Thank you, Katie. And thank you  
3 to the ComhrPssionfor yaveng fthis Trhyyou

1 limited in its distribution.

2 Then you fast-forward and think about the era  
3 of the PC and client server, and how that helped to put  
4 processing power on one's desk, not one's pocket, not  
5 one's car, but on one's desk. And how that distributed  
6 model resulted in a proliferation of servers, many of  
7 them kind of underutilized. They were only sitting there  
8 being called for certain uses and a lot more of a  
9 distributed model. That led to the growth of new  
10 companies and new industries, a new ecosystem.

11 Fast-forward again and what Danny Weitzner  
12 talked about, the internet and he came into policy in the  
13 '90s, and so did a lot of -- so did I, at least -- a lot  
14 of us here. And I would say that was the start of a  
15 dialogue that we are continuing this day. That's the  
16 emergence of what we now have put a name on. We put a  
17 name on it called cloud computing. But I would submit

ie only at that point the emergence of the Web and the ability to

- 1 altitude, you're changing location. And I think we
- 2 started walking in that forest in the '90s and the trees



1 you have a business customer and cloud computing  
2 customer, it's actually a much more participatory form of  
3 outsourcing than traditional business-process  
4 outsourcing, where an entire function is being handed to  
5 an outsourced company.

6 In many of the B2B cloud computing models,  
7 including my own company, the business customer actually  
8 controls the processing of the data in the cloud. So I  
9 just would like to put on the table that at least in the  
10 B2B context it's much more participatory with respect to  
11 the business customer than a traditional business-process  
12 outsourcing scenario.

13 MS. RATTE: So that will be interesting to  
14 discuss that model and how consumer-privacy interests  
15 could be protected in that environment.

16 Going to the issue of the ease of collection  
17 and the cheap storage of data, just posing as a general  
18 question right now to the panel, and we will get into it  
19 in more detail: Are we moving into a situation where we  
20 are taking away the incentive to delete data? And  
21 there's no incentive to -- it's more expensive to get rid  
22 of data than to keep it, and what impact might that have  
23 on the consumer-privacy interests here?

24 Beth, did you want to...

25 MS. GIVENS: Well, we keep track of data





1 organization, whether it's because of ediscovery or its  
2 data breach or other obligations or risks, to try to have  
3 better data hygiene. I don't think we can say that we  
4 are all the way there. Actually, I don't think  
5 organizations are yet. But I think that's a trend that  
6 is countervailing to the notion that storage is free,  
7 therefore there will be a proliferation. And it's one to  
8 watch. I don't know exactly how fast it will develop,  
9 but I see it happening in the marketplace.

10 MS. RATTE: Scott.

11 MS. OZER: Yes. Just a quick point. I think  
12 that the incentives, I mean you're talking about is it  
13 inexpensive to delete, and therefore do people keep it,  
14 but are there incentives to continue to use or find more  
15 uses, monetize that data. And we're seeing that, right?  
16 There's an emergence of advertising called behavioral  
17 targeting. Well, you know, most professionals in  
18 behavioral targeting spaces would tell you right now that  
19 'I don't know quite how I can use that data yet, but if  
20 you let me use it, then I'll find a way to use it and  
21 provide additional value.'

22 That argument is the same argument that we've  
23 heard in the fraud or the analytical-forensics spaces  
24 where a scientist in a fraud-research area will say, 'You  
25 know I don't know if that data will help me find a bad

1 pattern, someone doing something illegal. But I won't  
2 know unless I have the ability to analyze that data.'

3 So there are with the proliferation of data  
4 there is that incentive for certain types of practices to  
5 say, 'Yes, more data is always better than less,' to  
6 counterbalance, I think, some of Harriet's good points  
7 with some of the incentives to get rid of data and  
8 practice some good hygiene.

9 MS. RATTE: I think now I am going to turn it  
10 over to my Comoderator so we can delve into some more of  
11 these consumer-privacy interests and how we might go  
12 about identifying and protecting them in this context.

13 MS. BERGER: And I think we're on an excellent  
14 path to that. Putting aside for just the moment all of  
15 the data the may be used by fraud analysts and their  
16 desire for ever-increasing amounts of data at times, are  
17 there tools that cloud providers are using now to help  
18 encourage their companies, to the extent that their  
19 clients realize they may not need all the data that they  
20 have stored in the cloud, are there tools that are  
21 helping them realize, inventory their data better, and  
22 get rid of data they may not be using regularly?

23 MS. FINCH: Sure. From a business perspective  
24 it comes down to what our customers demand and what the  
25 regulations require. And some tools that are currently





1           We also found that the type of processing was  
2           changing because it was all networked. It was networked  
3           on a global scale. And then what Harriet was just saying  
4           a second ago is there's really been a change at least at  
5           the leading companies in the type of professionalization,  
6           the type of management that was going on. And so kind of  
7           the global answer to you would be how 0 a ss6id 7 on  
8           those good management processes?

9           And that actually reminds me of something Marty  
10          Abrams says, who's a privacy consultant, about if he goes  
11          to a meeting of privacy professionals and there are a  
12          bunch of companies there, he's kind of like Santa Claus,  
13          although that's not the comparison he uses, because he  
14          knows who's naughty and who's nice. And his metaphor is:  
15          I could if I had to pick out the companies that are  
16          really investing in professional-privacy management and  
17          those that aren't.

18          And so the at least kind of like I 7 professor  
19          answer to your question would be: Figure out a mixture  
20          of carrots and sticks so that ss6kind of do the Marty  
21          thing, where ss6are encouraging the set of companies  
22          that aren't in the good room to go there, but by doing  
23          that ss'll be incentivizing the companies that are  
24          investing in privacy protections to continue to do so,  
25          because companies are not just like black boxes. There

1 are people who are fighting for budgets and fighting to  
2 be able to convince their bosses that really we should be  
3 making this decision. So that would be my answer for  
that: CarBes eneets rLu.r

1 practices are.

2 As Harriet and I mentioned earlier, this is a  
3 form of a service provider relationship. And in all  
4 service provider relationships the service provider does  
5 not have that direct relationship with the end consumer.  
6 And that's what's really challenging about this model and  
7 all service provider models. But that's why I think it's  
8 so important for the cloud companies and the service  
9 provider companies to be transparent not only with their  
10 customers but with the ultimate consumer so they know who  
11 the good and bad guys are.

12 MS. BERGER: Nicki.

13 MS. OZER: In the business context it's nothing  
14 new that the company has been in possession of the data,  
15 but possession hasn't always equaled giving up control.  
16 So for ages consumers have stored their things with other  
17 companies. We have gone to people that have specialized  
18 skills to process that information. But just because we  
19 don't have possession of the item or the thing or the  
20 data does not mean that we have given up control and that  
21 we shouldn't have control over that information.

22 And I think what's made possible all of this  
23 being able to trust companies and individuals with our  
24 information is that there has been this trust and there  
25 has been this ability to retain control even if you don't



1 retain possession. And when ECPA was passed in 1986  
2 maintaining this kind of control was on the minds of  
3 Congress.

4 I found this quote from the Senate Judiciary  
5 record that said very clearly: "For the person or  
6 business whose records are involved, the privacy or  
7 proprietary interest should not change."

8 I think that's a really important issue because  
9 the core concept of making sure that just because you  
10 don't have possession, just because my information has  
11 gone to one company who then has shared it or has been  
12 doing services or storing it with many other companies  
13 doesn't mean that initial control shouldn't still reside  
14 with the initial consumer.

15 I think, as Harriet said, a lot of this is not  
16 new, the issues of possession and control, but there are  
17 some things that are quite new. You know it's not a  
18 surprise to anyone in this room that the efficiency of  
19 copying and accessing and mining and sharing data has  
20 increased astronomically in the past 20 years and that  
21 the business models have also changed. There is an  
22 incentive for companies to look to access this data, to  
23 mine this data, to share this data, and I think those are  
24 important issues we need to think about because the  
25 information is going to one company who may then share it

1 with another company who then might be subcontracting it  
2 to another company. And the original consumer likely  
3 doesn't know who those people are, what they're doing  
4 with it, what information they have, and what standards  
5 are being used to protect it. So you have got sort of  
6 layer upon layer of remoteness from the original  
7 consumer.

8           Some more collection and access and use is  
9 possible, but what I hope that we're here to discuss is  
10 there are things that are possible but what is  
11 appropriate and how are we going to strike the right  
12 balance between innovation and consumer protection in  
13 this area of cloud computing.

14           MS. BERGER: Very good. That is very helpful.  
15 And I think we do want to hone in on some types of  
16 mechanisms that might be helpful to assist consumers to  
17 have this type of control in this context, but, first,  
18 Harriet, I know you have been waiting.

19           MS. PEARSON: And it is actually exactly on  
20 that point about addressing the key issue, actually, that  
21 the consumer is interested in. And I just make one  
22 factual point and then a policy point.

23           And the factual point is that a cloud is not a  
24 cloud is not a cloud. You have various ways to tap into  
25 virtualized, distributed computing, and all the other

1 buzzwords, but basically there is this thing going on.  
2 The Web in the '90s and what we see as consumers made it  
3 possible to change how we communicate with one another  
4 and the kind of services that are provided.

5         What is going on right now is something in the  
6 infrastructure deeper down in the computing layer.  
7 That's changing. That's becoming more dynamic. And the  
8 provisioning of computing power, instead of being in one  
9 place and kind of rigid, is now more dynamic. So as that  
10 happens you can tap into that capability in different  
11 ways. So there's this concept of a public cloud which I  
12 think a salesforce would fall into, where you're tapping  
13 in, and other organizations and my own offer public  
14 clouds, where you basically rent the computing power.  
15 You have a large organization, an organization that is  
16 interested in tapping into that ability but concerned  
17 about keeping the data secure or the sensitivity of the  
18 workload, and they can create a private cloud and tap  
19 into that same computing model. And then there is a mix.

20         So I think it is important to understand the  
21 variety of the computing possibilities here. And then  
22 you can apply the analysis that says: Okay, if you are,  
23 for argument's sake, a large financial services  
24 institution and you are doing a private cloud, I do not  
25 know that the issues are that different from a consumer

1 perspective because you are still doing the same thing.  
2 You're just using a different back end. If you are a  
3 large organization or a small company and you are tapping  
4 into a public cloud, that may raise those issues.

5 And then the last policy point I will make is  
6 that I think we need to look at the policy issues through  
7 the lens of what is the use of the information, what are  
8 the services being provided, because you can have a  
9 healthcare organization tap into cloud computing to  
10 provide healthcare services, and you could have a bank do  
11 the same thing for banking, you could have a school do  
12 the same thing for educational purposes, and you get into  
13 this very quickly, the sectoral issue of what is the use,  
14 how do we best optimize the value and the innovation that  
15 comes from the uses and the efficiencies in that  
16 organization and the savings and the service-provided  
17 quality with the need to meet consumer expectations and  
18 protect individuals. And I think you quickly get into  
19 that analysis of kind of more of a services or the actual  
20 use of the model instead of the model itself.

21 MS. BERGER: Before we become too specialized  
22 in our discussion of the different context or types of  
23 cloud, can we talk about what is the role of transparency  
24 in the cloud? What about is something that consumers  
25 should be interested in knowing and what about is just

1 going to be what another panelist called today too much  
2 information about information, or what I like to call  
3 privacy TMI?

4 So does anybody want to address that, what do  
5 consumers need to know and why is it important?

6 Scott, do you want to start?

7 MR. SHIPMAN: Sure. The comment was raised  
8 which is what controls we provide for the consumer and  
9 now we're talking about either the cloud of the cloud of  
10 the cloud or how removed is it.

11 Sometimes it's helpful to look at examples.  
12 Paypal is a service provider not only for consumers but  
13 also for businesses who are looking to accept payments  
14 from their consumers. And as a Luxembourg bank Paypal is  
15 governed under bank secrecy. One of the things that that  
16 requires is that Paypal has to disclose their service  
17 providers, the service providers that Paypal uses.

18 And so in the Paypal privacy policy within  
19 Europe, because we're not a Luxembourg bank in the United  
20 States, there is a laundry list of all of the service  
21 providers that Paypal retains and have to use to process  
22 or further process the information. Now some of those  
23 are internally-made companies and many of those are  
24 external third parties.

25 And the question I would ask is: Okay, by law

1 they're required to provide that list, and we update that  
2 list ad nauseam. Right. I mean imagine every time we  
3 enter into a new agreement, we update our privacy policy  
4 in the appendix and we add another company to that list  
5 and the general or anticipated use that that provider can  
6 use the information for.

7 What additional value does that provide to the  
8 end consumer, if any, right?

9 MS. BERGER: Yes.

10 MR. SHIPMAN: I pose that question because, I  
11 think as Harriet was saying with her last comment on  
12 policy, which is if we were to adopt more of a holistic,  
13 use-based approach, so that we knew generally the service  
14 providers can only use the information to facilitate the  
15 service from which they have been retained, then does the  
16 consumer have a broad -- have we increased their broad

17 as Harriet was saying with her last comment on

1 be good and would give consumers opportunities that they  
2 might use?

3 Nicki, you've had your card up for a while.

4 MS. OZER: Well, I think there is a limitation  
5 sometimes to notice when notice doesn't actually give you  
6 information or give consumers information that is helpful  
7 to them in making an informed decision. But we spent  
8 some time, the Technology and Civil Liberties Team at the  
9 ACLU of the Northern California, in the past couple weeks  
10 looking to sort of see what kind of information do  
11 consumers really know about companies and what kinds of  
12 other companies they are working with in terms of storing  
13 data or processing data. We didn't have a lot of time,  
14 but looking at some of the top companies it is pretty  
15 clear that consumers don't have very much information  
16 about who these companies actually work with, what kind  
17 of information these companies are storing or processing,  
18 where these companies are, or what the data practices  
19 are, or how this information is protected.

20 We get really general comments like: 'We  
21 provide such information to our subsidiaries, affiliated  
22 companies, or other trusted businesses, so don't know who  
23 these folks are. We require that these parties agree to  
24 process such information based on our instructions and in  
25 compliance with this policy and any other appropriate





1 content of data when we may determine it to be necessary  
2 or desirable.' Okay. Or things like, 'We may access or  
3 disclose your personal information, including the content  
4 of your communications.'

5 Some companies, like Salesforce, gives notice  
6 to its primary company, which we did not even see in a  
7 lot of these. So notice is great, that I should know who  
8 these companies are and what they're doing with it. But  
9 there also need to be real standards set in place and  
10 those need to be communicated to the consumer.

11 MS. BERGER: These are good contrasting  
12 examples. You maybe don't want a Luxembourg list of  
13 service providers, but some of the general language, I  
14 think you had a lot of like sympathetic laughter, we've  
15 all seen general language like that before. So where is  
11 the sweet spot? What do we need to

1 consumer is that does not necessarily get you there. And  
2 I think there is a real issue with the TMI.

3 And, to give you an example, so when I did the  
4 white paper for Richard Purcell, we had six leading North  
5 American global companies, they were anonymous. We  
6 gathered information for the case studies. And they told  
7 me a lot about how they manage global data flows,  
8 dynamically routing by algorithm. And after a while even  
9 though I was the expert it was like: Guys, like stop. I  
10 can't take it in anymore, and I have to do the report and  
11 I supposedly know about this kind of stuff. And there  
12 were more details and more details.

13 And so the reality is the basic consumer,  
14 whether you are imagining your mother or whoever it is,  
15 they will beg you to stop sharing the information, which  
16 doesn't mean that the FTC shouldn't have a sense of what  
17 the right B2B contract is.

18 The other thing is something that Nicole said  
19 that is very important that I think should be a go, she  
20 used the word "responsibility." And so if you want to  
21 move the companies into the Marty Abrams good-guy room,  
22 you have got to figure out how to make them responsible.  
23 And I think a big thing that comes with that is  
24 liability.

25 The final thing, Fred Cate has a great

1 presentation that he gives about flows and notice and  
2 choice. And my only regret is that it is not available  
3 right now on YouTube because I think for the week it  
4 would be the most-watched YouTube, ahead of the Stupid  
5 Pet Tricks or whatever people are watching on YouTube  
6 now.

7 And Fred is really very, very convincing about  
8 the problems kind of currently of notice and choice. So  
9 I think it is important then if we want to protect  
10 consumers at the end of the day, to figure out how do we  
11 do that.

12 MS. BERGER: So now is our chance. I think my  
13 panel is getting -- you're getting way ahead of us here.  
14 You are talking about the mechanisms for delivering the  
15 notice, you might have consumers looking at the B2B  
16 contracts, but what do we know that we really want to  
17 inform consumers about? I want to stick with that first.

18 What is actionable for consumers? I know one  
19 thing people raise a lot is the potential for secondary  
20 use, that information stored in the cloud might be  
21 subject to a secondary use.

22 First of all, let's comment on that scenario.  
23 And then, second, if that is the case or to the extent  
24 that it is, how would you let consumers know about it or  
25 give them an opportunity to take an action?

1 Lindsey.

2 MS. FINCH: The issue of secondary use I think  
3 is an interesting one because it's not always clear  
4 exactly what is a secondary use. So we think of the  
5 primary use as being the use that is disclosed to  
6 consumers when their information is collected. That  
7 notice that is given. That is how their information is  
8 going to be used, but sometimes that is extremely  
9 overbroad.

10 But for the moment I will assume that secondary  
11 use is a use of the information that a consumer would not  
12 necessarily expect when they hand that information over  
13 to the initial collector and user of that information.

14 In the cloud it really varies contract to contract,  
15 provider to provider, and to really look and see. To the  
16 extent a company is acting as a service provider or, to  
17 use the European terms, the data processor rather than  
18 the data controller, then that entity should only be  
19 using the data as instructed by the data controller or  
20 their customer company.

21 And I would be looking for terms in a contract  
22 that say the data is only going to be used for those  
23 purposes. So you really need to look at how the  
24 information not only is going to be used but when the  
25 information can be accessed, when the information can be

1 disclosed. So those would be some standard terms that I  
2 would be looking for in a B2B contract with a cloud  
3 provider, because it really depends on the model right  
4 now, but I think there is room for self-regulation here  
5 and possible enforcement if there is going to be uses of  
6 information that goes beyond what that contract is  
7 between the cloud computing provider and their customer,  
8 and then going back to that original notice that the  
9 business customer has given to consumers.

10 MS. BERGER: And I want to get Beth's views too  
11 on what consumers need to know about the use of their  
12 data in the cloud or the handling of it in the cloud.

13 Thank you, Lindsey.

14 MS. GIVENS: Oh, yes, and then speak to a  
15 secondary use as well?

16 MS. BERGER: Yes.

17 MS. GIVENS: Well, to lead off from what Nicole  
18 said about fuzzy terms, and I guess I could even say  
19 cloudy terms, but the difficulty of figuring out what is  
20 going on in a privacy statement or a policy statement,  
21 there are many consumers who actually need to know the  
22 details of what is happening to their data as Company X  
23 hands it off to Company Y. In extreme cases there are  
24 stalking and domestic violence victims who will certainly  
25 want their address to be protected. They should also

1 know that in a cloud environment there are lower legal  
2 standards for search and seizure. So there are issues  
3 like that I think it would be good for consumers,  
4 especially those with particular needs, to know about.

5 So Company X contracting with Company Y, I  
6 think Company X should tell the consumer and give them  
7 enough information about their dealings with these third  
8 parties that they could make informed decisions, that it  
9 would be good to know things about the company's  
10 stability, for example; access provisions, deletion  
11 provisions, how do you get your data out; customer  
2 service points of service, how do you 1111111111111110; cn;-ndards for semo  
2

1 health information. Some of this, this is vast amounts  
2 of information, some of it very sensitive to who we are.

3 And I do not want to overstate how much notice  
4 people should get and, I think as our Moderators know,  
5 that I certainly think that notice is limited, notice is  
6 not protection, but I think it would be good for folks to  
7 know what kind of information is going where and, with  
8 that, what kind of standards there are for the protection  
9 of that information, because I may not want to do  
10 business with somebody and give them my health  
11 information if they are then subcontracting with a  
12 company that is then going to be disclosing that  
13 information under very lax standards. So I think these  
14 pieces of notice have to go together about who the  
15 companies are, what kind of information it is, what  
16 standards there are, and of course those standards need  
17 to be a whole lot stronger than they are right now. But  
18 it all goes together as a package and I think those  
19 pieces are very important together.

20 MS. BERGER: Okay. This is good and I want to  
21 hear also from you, Harriet, and then we can maybe look  
22 at some of the mechanisms through which you might deliver  
23 this information to consumers and how that might be  
24 accomplished. Harriet.

25 MS. PEARSON: Let me try to take us back a





1 in an organization, we have an HR department. The HR  
2 department has a lot of information about us. The HR  
3 department is probably outsourcing and contracting with  
4 one or two companies. And, in turn, that set of  
5 companies is outsourcing to probably another set of  
6 companies. And they all have information about you that  
7 relates to the provisioning of health benefits,  
8 disability, maternity leave, adoption assistance,  
9 whatever the set of benefits or HR processes that you get  
10 from your organization, chances are, are probably no less  
11 than half a dozen to two dozen companies have information  
12 necessary for the provisioning of those services. That  
13 is happening independent of whether a private or a public  
14 cloud is being used.

15 And the question is as we evolve to more  
16 dynamic provisioning of computing power, whether the  
17 underlying issues we have been asking ourselves for  
18 decades now and we are going to continue to ask  
19 ourselves, which is 'I need to know, I should know,' but  
20 the question is: Well, so what should HR do? Should HR  
21 then keep a running track to Scott's point of all the  
22 providers and then update it, make sure you know? That  
23 doesn't seem practical or workable or even that valuable.  
24 And then it's this balance.

25 And that balance, I submit, can be struck at

1 some place and level probably but also needs to be kept  
2 in mind the type of activity, that the healthcare  
3 situation is different from other situations. And we  
4 already have a rich history and enacted law in this  
5 country that informs the policy decisions that we and the  
6 Commission and others would take.

7 MS. BERGER: Okay. Scott, did you want to  
8 comment on this?

9 MR. SHIPMAN: Well, you wanted to focus on  
10 mechanisms, and so I was ready to get there if you wanted  
11 to get there.

12 MS. BERGER: Yes. Please.

13 MR. SHIPMAN: It is a bit of a transition even  
14 from what Harriet said with the list. And there is an  
15 expectation I think that we might be off on, which is  
16 that an individual whose data is being processed, whether  
17 a consumer or an employee, they want to know all of this.  
18 And I would posit that they do not want to know any of  
19 it.

20 Right now I think Beth raised some good points  
21 about certainly if you have sensitive personal issues, if  
22 there is an expectation the information could be used in  
23 a harmful way, well, then certainly that is something you  
24 would want to know, except most likely if they are going  
25 to use it in a harmful way they are a bad actor and they

1 are not going to tell you anyway.

2 So rather than focus on all of this notice and  
3 disclosure that we have focused on for ten years, I would  
4 argue that maybe we should look at some norms or some  
5 standards, use-based norms or standards a little bit  
6 relating back to the point I was making earlier, which is  
7 to say there is a default presumption of how information  
8 can be used. If you're a service provider there is a  
9 default presumption as to the types of typical uses that  
10 are considered typical, primary.

11 And if there are additional uses that aren't  
12 typical or primary, that then there are additional  
13 notification steps, there are additional transparency or  
14 choices that need to be imposed depending on the type of  
15 data.

16 Now a lot of this work is being done and has  
17 been done over the last three or four years with the  
18 Business Forum for Consumer Privacy that Marty Abrams and  
19 team have been pushing forward. And that is what is  
20 referred to as the use-based approach. Because, again,  
21 if I am a consumer, do I really want to know all of the  
22 service providers that Paypal uses and then do I want to  
23 have a right to be able to ask for the business-to-  
24 business service provider agreement to check the  
25 encryption level and the standards just to feel good?

1           And, on the flipside, in many cases while  
2           Paypal is a larger organization, so many of the small  
3           businesses of the world do not have any negotiating power  
4           against, to Harriet's example, any of the HR or large  
5           organizations that actually are the service providers,  
6           right, --

7           MS. BERGER: So okay -- okay.

8           MR. SHIPMAN: -- so you can't negotiate. So  
9           you are stuck with whatever policy the big service  
10          provider is going to provide to you, but you are the one  
11          that looks bad because you have to provide the notice to  
12          the consumer.

13          MS. BERGER: So in terms of establishing these  
14          positive norms for the delivery of these services,  
15          Lindsey, I know you can talk about the negotiation of  
16          these contracts, and hopefully some others can talk  
17          about, well, what should be them. If that is going to be

1           Imagine if you were to be overwhelmed with all  
2           the information of all the service providers they use, to  
3           build on the points made by other panelists. What I  
4           would want as a consumer is to put that company that I  
5           directly do business on on the hook for any service  
6           provider relationship that they have down the chain.

7           So what I would argue for is I think there  
8           needs to be an open discussion about what these use  
9           standards are, pulling on the examples that Harriet and  
10          Scott raised. But the service providers then need to be  
11          accountable for assuring that those standards are upheld.  
12          But it's that initial company that the consumer has the  
13          relationship with that needs to be on the hook for that.  
14          Because just thinking of the number of financial  
15          institutions that I do business with, I can't imagine  
16          having to ensure that all of their contracts are upheld  
17          and upheld.

18          So what I would argue for here is, yes, we do  
19          need to definitely have a conversation about what  
20          appropriate uses are, but that it's that original company  
21          that needs to make sure that those flow through in the  
22          contracts with their service providers.

23          MS. BERGER: And before I take the follow-up on  
24          that, we have a audience question who -- people may not  
25          be quite ready to move on from the idea of informing

1 consumers. And the question is: Is it more important  
2 for cloud computing to provide notice about disclosures,  
3 who they share with, or what they share or where the data  
4 are stored?

5 What are the most -- I guess it is not coming  
6 across that we have satisfactorily covered that topic.

7 Yes.

8 MS. RATTE: Yes. The way the question is  
9 posited, do you want to give notice about the types of  
10 things Scott was talking about: The service providers  
11 that you use, who you share it with. Or should the  
12 disclosure be more along the lines of what due diligence  
13 is applied and what you do to monitor that your  
14 procedures are being followed?

15 MS. OZER: I would say notice puts the burden  
16 on the consumer for self-protection. It is not  
17 protection. It puts the burden on us to protect  
18 ourselves. And these are very complex issues that we  
19 don't necessarily understand. We already realize most  
20 people either don't read or don't understand the privacy  
21 policy. So I do not say that -- you know notice has  
22 great limitations to it. I do not think that it is the  
23 solution to this, but I think the solution is for there  
24 to be good protections on use, retention, deletion, and  
25 on disclosure, so that there are strong standards across

1 the board.

2 I think that often in the public-interest  
3 community when we do not have these stronger standards,  
4 when regulatory action has not been taken by the FTC or  
5 actions by other places, notice at least can create some  
6 of the knowledge to push this change. So I think that is  
7 why sometimes we talk about notice because when there is  
8 no notice there is no transparency. And then no one  
9 understands what's happening and then there isn't the  
10 kind of energy and ability to create change, because  
11 people will say, 'Well, what's the problem? How do you  
12 know there is a problem? Why should there be a fix for  
13 this when you don't even know there is a problem?'

14 So I think the burden shouldn't be on the  
15 consumer. The burden should be on having the right  
16 standards. And I cannot agree more with Lindsey on the  
17 fact that that needs to go through the chain and, as the  
18 Commissioner noted this morning, there has to be that  
19 custody of control throughout the entire chain of cloud  
20 computing.

21 So we are hopefully going to get to this more  
22 at the end in terms of more solutions, but I think use,  
23 retention, deletion, and disclosure are all important  
24 pieces that we need to think of in terms of standards  
25 and better protections for consumers.

1 MS. BERGER: Consumer interest to protect,



1        seen is something called desktop virtualization, which  
2        sounds pretty gorp, but it just has to do with lots and  
3        lots of desktop computers. And you get the ability to  
4        save lots of money by virtualizing or serving out that  
5        computing power instead of having computing power at  
6        every desk.

7                Efficiencies are there. You do it usually  
8        within an organization. And there is personal data,  
9        personal information involved in that, but not -- not to  
10       the point where it would say, okay, what is the consumer  
11       effect of that. So I just throw that out as an example.

12               Another one is what is known also as server  
13       consolidation which goes back to that other era of  
14       computing. We had lots and lots of servers. And they're  
15       underused and they're turning and they're using up  
16       energy. And what people have been finding is that they  
17       can save a lot of money and a lot of CO by consolidating

1 operations is the one that has the relationship with end-  
2 consumers. Then you get back to the same issues we've  
3 been wrestling with.

4 MS. BERGER: I want to focus a little bit on  
5 advancing the same discussion. Do consumers even know  
6 what the data is at this point? If it's all being  
7 processed and aggregated in the cloud and managed in ways  
8 that they may not precisely anticipate, do they even know  
9 what the data is? Do they need some form of access to  
10 the data to know what's even in the cloud?

11 Paul, did you want to speak to that?

12 PROFESSOR SCHWARTZ: Well, I am still kind of  
13 struggling with the notion the consumer, and again the  
14 fact that there is a reason why we want to have  
15 information out there, and to the extent that you have  
16 some consumers who care about it, it may that one in a  
17 hundred will carry that task, but in a way the real task  
18 is what are we trying to accomplish?

19 So kind of cutting apart from the consumer,  
20 that for me is the big question, and I think what we want  
21 to do is move to a sense of reasonable practices are for  
22 the cloud and then try to move industry over time, the  
23 same way we do in tort for dealing with a whole variety  
24 of industrial accidents, so how do we get to reasonable  
25 practices so that industry moves there and so that it

1 evolves, so then in ten years -- and I have an answer.

2 MS. BERGER: Nicki has suggested that one of  
3 the ways we evolve our norms for what reasonable  
4 practices are is by learning consumers' reactions when  
5 they are informed of the practices. So how do we get  
6 there? How do we get to that spot?

7 PROFESSOR SCHWARTZ: Well, okay, and I also  
8 have a problem with that in that I can understand if it's  
9 1920, that we have a reasonable expectation involving all  
10 kinds of things. The difficulty in terms of the  
11 consumer's reasonable expectation is that there is so  
12 little time for that to form and the sense of a community  
13 is so different today. So how do you develop an informed  
14 kind of community expectation about Paypal, about  
15 Facebook, about Salesforce if a second ago it didn't  
16 exist and now it is millions and millions of people on  
17 Facebook?

18 So again I would say this is the thing: Can we  
19 decide, however that happens, what the reasonable  
20 practices are that we want to have over time? Then I  
21 think it is going to be a mixture of mandatory guidelines  
22 from government, negotiated guidelines, whether COPA is a  
23 good example or not, maybe some naming and shaming by  
24 government of companies that fall short. And then I  
25 think a big factor here is adequate liability, because

1       there are all kinds of things in life we should be doing,  
2       maybe like being a little more careful in sorting plastic  
3       bottles and looking at the bottom, whether it is a 5 or 6  
4       and going back to what the regulations are in our  
5       community, which we may not do. But if there is  
6       liability, we care about it.

7               So then the big question in terms of liability  
8       is thinking about private rights of actions, thinking  
9       about class actions to lead it back to the consumer  
10       because it is going to be maybe one consumer in 2000 that  
11       actually cares about it. And if you can't then bundle  
12       those consumers together or if those consumers are only  
13       going to get a nickel at the end of the day, you are not  
14       going to move people to reasonable practices.

15              MS. BERGER: And so we heard a lot earlier in  
16       the day about how what I think someone said, transparency  
17       being a powerful light to shine on the dark void of data  
18       collection, so there seems to be some discussion today or  
19       some thinking today that incentives are created by  
20       transparency and not just by the threat of liability.  
21       And there was also a lot of emphasis this morning on the  
22       idea of consumers having access to their own data when  
23       they are directly interacting with a company.

24              So let's not forget that a hold at a cloud  
25       company is only holding the data on behalf of another



1       happened. But I agree that there are a lot of  
2       limitations to the ability for consumers to absorb this  
3       type of information and then to engage in self-  
4       protection, because there are limitations to that.  
5       That's not really the position that we want consumers to  
6       have to be in.

7               MS. BERGER: I think we have talked about this  
8       a little bit already, but does the cloud provide an  
9       opportunity? The cloud service and the sophisticated  
10      analytical tools that are often present in the cloud,  
11      does that provide an opportunity for consumers to learn  
12      more about how the companies they do business with are  
13      handling and collecting their data?

14             Lindsey, can you talk to that?

15             MS. FINCH: So, just to step back for a minute,  
16      you know at Salesforce's contracts we say, and this is  
17      just in our standard agreement, that we are not going to  
18      access customer data, that is, information that our  
19      business customers submit into our service except under  
20      very limited circumstances. So it would actually be a  
21      violation of our contract to provide direct access to a  
22      consumer information that one of our customers has stored  
23      about them.

24             But that being said, through our membership  
25      with Safe Harbor, if we were to receive a complaint from

1 an individual, we would have to work with the business  
2 customer to resolve that dispute.

3 But I do think that, just to kind of, again,  
4 back up to some of the discussions we were having earlier  
5 about the massive amount of information that is being  
6 kept right now and that is not being deleted because the  
7 cost of storage is cheaper than the cost of deletion,  
8 organizations and even individuals are being overwhelmed  
9 with data. Data clutter, I mean it is overwhelming. And  
10 tools are being developed to help us deal with that.

11 To give a couple examples. So Facebook, I have  
12 a couple hundred friends on Facebook, probably a hundred  
13 that are very active posters. Facebook provides me  
14 mechanisms to sort of filter through the noise. I can  
15 look and see these are the status updates I want, so it  
16 gives me a means of dealing with that information.

17 Another example, there is a company called  
18 Xobni, it's "inbox" spelled backwards, that helps you to  
19 deal with the email clutter that you get so that it can  
20 prioritize and help you rationalize the email you get.

21 I think what the cloud can do in this space is  
22 to help to provide tools to help companies better  
23 understand their information so that, in turn, they can  
24 provide better information back to their consumers. So  
25 it's a rather indirect answer to your questions, but I

1 think the cloud computing technology can certainly help  
2 their business customers get there to better serve  
3 consumers.

4 MS. BERGER: And so in terms of those  
5 analytical tools providing an example for a way to help  
6 consumers, you also mentioned the dispute resolution --

7 MS. FINCH: Yes.

8 MS. BERGER: -- for the safe harbor. And I  
9 think that is a great segue to the topic that Katie is  
10 now going to lead us through in terms of data  
11 cross-border transfers.

12 MS. RATTE: Yes. And before we turn back to  
13 the international dimension of this computing model,  
14 stepping away from calling it a business model, see if  
15 Paul and Scott have comments on the last discussion  
16 first. We'll start with Scott.

17 MR. SHIPMAN: Sure. Specific examples, you  
18 know we heard on the previous panel that privacy, there  
19 was robust competition and that it was a market  
20 differentiator for a number of companies. I think that  
21 is also true in this space.

22 When you are looking at -- again, to take a  
23 specific example, you can have mom-and-pop businesses  
24 processing credit cards, accepting payments, trying to  
25 become PCI compliant, and dealing with all of the



1 collection of sensitive information in a very poor or  
2 low-tech way, or you can use an online-payment service  
3 provider, one that I happen to work with, that does all  
4 of that for that mom and pop. And so it does a number of  
5 things.

6 It takes the data out of the hands of a less-  
7 sophisticated operator. It enables financial and  
8 regulatory compliance, focused on one area of expertise.  
9 Now some would argue that it also creates a security  
10 vulnerability by having data all in one location rather  
11 than a distributed model. But it's an example of where  
12 if you were to take that and, say: Yes, and let's add a  
13 use policy, let's add retention policies, let's lead as a  
14 service provider because it will be a market  
15 differentiator for us. Businesses will want to use our  
16 company because we make their privacy compliance easy,  
17 right?

18 So it is the same step that Nicole was saying  
19 at Google where they are constantly innovating and using  
20 privacy as a competition piece directly with the  
21 consumer. But in a B2B world it's the exact same story.

22 MS. RATTE: Paul.

23 PROFESSOR SCHWARTZ: Yes. I want to make two  
24 quick points. To follow up on something that Beth said  
25 before that I thought was incredibly valuable was raising



1 that you have these kinds of passwords, you have this  
2 kind of encryption.

3 Then the same thing with controls, which I  
4 think allowing people to control information is very  
5 important, but all of a sudden you can have someone  
6 changing someone's medical record or changing who that  
7 record can be shared with. So it is a kind of the  
8 department of be careful what you wish for, although I  
9 think it is a very important point.

10 MS. RATTE: Right. I think the authentication  
11 point is critical when we are talking about things like  
12 access because of the other dangers that you raise.

13 I want to go back for a second to something  
14 that Lindsey brought up which is dispute resolution,  
15 particularly when you're talking about in a cross-border  
16 context. In fact we got a question from the audience  
17 that sort of speaks to this issue. "What legal recourse  
18 does a consumer have if their data is compromised in the  
19 cloud, particularly if the data are stored in another  
20 country?"

21 So I wonder if some of the business folks on  
22 the panel could sort of speak to how you handle this  
23 issue and how we ensure that that sort of jurisdictional  
24 risk doesn't just land on the consumer. Scott.

25 MR. SHIPMAN: Well, you know the first question

1 is where is the consumer, right? I mean if the consumer  
2 is in the EU and they are dealing with an EU company,  
3 well, they absolutely have a right of recourse.

4 In fact if they are consumers in the EU and  
5 they are dealing with a U.S. company and the U.S. company  
6 has any location in the EU, they have a right of  
7 recourse.

8 Now is that class action, is that no proof of  
9 harm? No, but they have the ability to have the problem  
10 remedied, right, and that is through the data protection  
11 agencies and the different country-by-country approaches  
12 that they have under the directive there that are, at  
13 some level or another, harmonized.

14 From a U.S. perspective, I think the closest  
15 level of recourse that we have attained to date would be  
16 in probably a few sectoral areas, like security breach.  
17 But with security breach the individual has the ability  
18 to receive notice and then obviously could pursue  
19 recourse with the company that they're doing business.  
20 But in fact if you look at the litigation record, there  
21 is not a single case yet where someone has successfully  
22 sued for identity theft from a security breach. It is  
23 rumored that there are a number of settlements that are  
24 not public, but there is not a single case out there that  
25 I am aware of where they have actually been successful.

1           And so that either points to either a lack of  
2           harm, but that is not entirely the case because we do  
3           know, in fact, it does take hours if not months to remedy  
4           an actual true identity theft. So there is some harm  
5           there, it just has not been successful yet.

6           MS. RATTE: Do you think there are other  
7           consumer-privacy interests, particularly things like  
8           access? We were talking about if a consumer is trying to  
9           get access to data that may be held in another  
10          jurisdiction, are there rules that should be in place  
11          here in the U.S. to ensure those types of protections for  
12          consumers? I am talking about in addition to the  
13          security-breach context that you are talking about.

14          MR. SHIPMAN: Sure. I mean I can speak, it is  
15          a little bit back to the previous panel, it is more in  
16          the direct-consumer-to-business model. In a consumer-to-  
17          service-provider model I think that is a much tougher  
18          question.

19          As Lindsey said, the primary conduit for access  
20          or for any type of rights, grievance, or questions should  
21          be with the entity that the consumer or the data subject  
22          has a relationship with. But in the business-to-consumer  
23          model I think one of the approaches that we are seeing  
24          emerge and certainly an approach that eBay has just been  
25          approved on is the binding-corporate rules approach that

1 Europe has adopted.

2 Take it out of the concept of Europe for a  
3 second and just say it is an opportunity that allows a  
4 company to say, "these are the standards that we are  
5 going to follow, irrespective of largely what law  
6 exists." And so for a company like eBay that means that  
7 we do provide access. And now certainly we are a new age  
8 company, so access is not incredibly difficult. For most  
9 companies it is a show-stopper. They simply couldn't  
10 provide the level of access that we can provide because  
11 our information has been collected digitally. So I mean  
12 that is an example, I guess.

13 MS. RATTE: Yes, that is very helpful.

14 Lindsey, do you have something to add there?

15 MS. FINCH: Yes. I think echoing what Scott  
16 said about binding-corporate rules, you know with the  
17 safe harbor, I know a lot of multinational companies that  
18 self-certify to the safe harbor framework do not limit  
19 those commitments to European individuals. So I know my  
20 company and a lot of other companies that are represented  
21 in this room that adhere to the safe harbor make that  
22 their global policy. They incorporate that in their  
23 privacy statement whether it is with respect to European  
24 individuals, U.S. individuals, individuals in India,  
25 Japan, you name the country. So that is sort of a not-

1 quite-so-binding-corporate-rule-like way of doing things,  
2 but it is an analogous approach where you are taking  
3 binding-corporate rules being based mostly on European  
4 law, you are taking the same concept with the safe harbor  
5 and applying it globally.

6 MS. RATTE: Right. Harriet, do you have  
7 something?

8-2.2732 TD ( MS. PEARSON: 4-4-04 TD (5), Just all concrete

1 consumer, and then what goes on behind that is kind of  
2 not really -- there is recourse directly to that, to the  
3 entity.

4           So I think this is another one of these where  
5 the scale of the use and the scale of the international  
6 transfers may be causing us -- and appropriately so, by  
7 the way -- to revisit and say now let's really think  
8 about this because more, more people will be involved in  
9 it, not maybe larger organizations that have the  
10 wherewithal, but maybe more. So we have got to think  
11 through that. And so there are probably mechanisms to do  
12 that.





1 line.

2 MS. FINCH: Well, I would just say that I know  
3 it is off the top of what we are supposed to be talking  
4 of in this panel, but with respect to security I think  
5 there can be a lot of standardization. I think there are  
6 international standards out there that can be followed  
7 because a lot of the things we have been talking about,  
8 not all of them, but a lot of them can be remedied  
9 through good security.

10 So I would propose things like self-regulation  
11 and working towards standards like ISO 27001.

12 MS. RATTE: Great. Thank you.

13 Beth. And, Beth, you have already shared with  
14 us a number of good substantive things there, so.

15 MS. GIVENS: Well, just in general I am a  
16 believer in the fair information principles, but I have  
17 my likes, those that I think are better than others, I  
18 think the Canadian set is my favorite, followed by OECD  
19 in terms of being robust.

20 I am heartened to hear that the Federal Trade  
21 Commission, I guess, is revisiting the whole issue of  
22 privacy principles. And I am glad to hear that because I  
23 do think there are some good models out there, but  
24 notice, choice, access, and security, that's not enough.

25 MS. RATTE: Nicki.

1 MS. OZER: Well, we said a lot in here. (Holds  
2 up publication.) I still encourage anyone to get a copy  
3 of it if you have not already. And in our FTC comments  
4 as well.

5 But I think just one really important area is  
6 the standards for disclosure to third parties. I think  
7 that whether it be in the enterprise context or in the  
8 more consumer context, it is very important for consumers  
9 to be able to trust that their information is safe and  
10 that there needs to be higher standards for disclosure.

11 Sensitive information should not be disclosed without  
12 judicial oversight. I think that is an area that public  
13 interest groups and businesses and government should

12 hopefully all be able to work together on. I know that TD (13 )Tj 2.8415 - FD (13 ),( interest groups and b

1 governmental and industry activity on the uses that we  
2 think are particularly pernicious, harmful, or just  
3 wrong, and trying to address those I think would may be a  
4 good frame to try to approach prioritizing.

5 PROFESSOR SCHWARTZ: I would say there is a  
6 continuum here and one end you have command and control,  
7 which might not be suitable anymore, where the government  
8 just kind of micromanages every algorithm, and then on  
9 the other end of the continuum is there is self-  
10 regulation of the kind we've seen maybe a decade ago  
11 where it means industry is kind of going to do what they  
12 want and call it self-regulation. So I think in between  
13 that --

14 (Laughter.)

15 PROFESSOR SCHWARTZ: -- and in between it is  
16 where the action should happen today. And so I think  
17 there is going to be room for negotiation of regulations,  
18 but I think there is a need ultimately for the FTC and  
19 other sectors of the government to have a sense of what  
20 should be done, and a normative standard that they then  
21 allow industry room around so they can figure out the  
22 most efficient, cost-effective, and reasonable way to do  
23 that.

24 MS. RATTE: Scott.

25 MR. SHIPMAN: Well, I have said it before and

1 actually said it in 2006, we have had guideposts. This  
2 is getting more and more complicated. We have got more  
3 and more data, moving faster. And I think that while  
4 many are opposed to actual federal regulation, I think  
5 that it will provide clarity that will help business, not  
6 hurt it.

7 Now of course the devil is always in the  
8 details and people become immediately skittish when you  
9 say we need actual laws rather than self-regulation. But  
10 there are a number of companies out there that have come  
11 to that realization and are working on that use-and-  
12 accountability model that I think has come a long way  
13 since '06, certainly it will take probably equally as  
14 long for it to ever happen, if not longer, but...

15 MS. RATTE: All right. With that note it's  
16 time for a 15-minute break. Please join me in thanking  
17 this very distinguished panel.

18 (Applause. Recess taken from 3:02 p.m. to 3:18  
19 p.m.)

20

21

22

23

24

25



- 1 and play music and store photographs and video. We can
- 2 take pictures. We can play games. We can work on the

1 mentioned carrier this morning, "You have zero privacy...  
2 Get over it" sound almost quaint.

3 In addition, questions have arisen about how  
4 effectively the existing privacy frameworks, particularly  
5 the notice-and-choice model, map onto the smaller screens  
6 of mobile devices.

7 All of this warrants serious public debate.  
8 That is why we are delighted to welcome our terrific set  
9 of panelists here today. With us we have, in order:

10 Michael Altschul, with us today from CTIA-The  
11 Wireless Association;

12 Kevin Bankston, to his left, Senior Staff  
13 Attorney at the Electronic Frontier Foundation;

14 Darren Bowie, Legal Director of North America  
15 for Nokia;

16 Alissa Cooper, Chief Computer Scientist for the  
17 Center for Democracy and Technology;

18 Amina Fazlullah, Counsel for U.S. PIRG;

19 Brian Knapp, Chief Privacy Officer and General  
20 Counsel for Loopt; and

21 Kristine van Dillen, Director, Industry  
22 Initiatives and Partnerships for the Mobile Marketing  
23 Association.

24 So we have a terrific and very-accomplished  
25 panel today, experts in their field who can help us to



1 delve into some of the thorny issues in this space. We  
2 will use the same groundrules for this discussion as we  
3 have for previous ones today, so this will be a moderated  
4 discussion.

5 We will call on you panelists in turn. You  
6 should also feel free to contribute to the debate at any  
7 time, ideally by holding up your table tent or setting it  
8 on end so that we know that you're interested in pitching  
9 in. We do have a lot to cover in an hour and 15 minutes,  
10 and many, many issues and subissues that we want to drill  
11 down into.

12 We do welcome questions from the audience. I  
13 know that there may be some frustration. We've heard a  
14 little bit of feedback on the Privacy Roundtable email  
15 address. The people are frustrated that not all the  
16 questions are being escalated. I can assure you that  
17 they are being kept, that the staff will be looking at  
18 those and will be considering them seriously. There  
19 simply is not enough time in every instance for us,  
20 frankly, to even get to all the questions that we have  
21 been working on for the last eight weeks. So we will do  
22 our very best. Do not be discouraged. Submit them to  
23 the [privacyroundtable@ftc.gov](mailto:privacyroundtable@ftc.gov) address.

24 If you have questions in the audience, somebody  
25 will be going around at about the halfway mark and a few



1 have in cellphones. So you have got cameras and you have  
2 got video cameras and you have got speedometers,  
3 accelerometers, and et cetera. So I think when we start  
4 looking at all of the different inputs the mobile phone  
5 has, you can start considering that not only do you know  
6 where you are, you know how fast you are going and which  
7 direction you are facing, so that is kind of interesting.

8 Another thing in the mobile arena is the role  
9 of the carriers. And this gets a little bit interesting  
10 in that in addition to being kind of the primary function  
11 of the customer service provider, they are also the  
12 biller. So they are providing the billing function.  
13 And, at this point, they are still the primary customer-  
14 facing brand. So all of the situations that occur on the  
15 phone, even the applications that are being downloaded,  
16 the consumers are really looking at the carrier when  
17 anything goes wrong; or if any information gets out about  
18 them, the carrier is perceived to be responsible on that  
19 area.

1 of their mobile phone interacting, they can be  
2 interrupted.

3 So those are the primary differences.

4 MS. HARRINGTON-MCBRIDE: Okay. Other thoughts?

5 Darren.

6 MR. BOWIE: One thought that is useful to make,  
7 Katie, is that there are number of different mobile-  
8 operating systems. And this is a difference from the  
9 online space, where there are not as many. So, for  
10 example, Nokia uses a Symbian operating system. There is  
11 a Microsoft operating system, Android, Apple, et cetera.  
12 While these provide a lot of choices and opportunities  
13 for consumers. Technically it can make it challenging to  
14 come up with one unified approach to technical solutions  
15 to privacy, for example. So that's just a fact that the  
16 current different mobile operating systems play a role  
17 here as well.

18 MS. HARRINGTON-MCBRIDE: Another way that that  
19 fragmentation issue plays out in this space.

20 Michael.

21 MR. ALTSCHUL: Well, when we are talking about  
22 the fragmentation, and earlier panels talked about the  
23 evolution of computing and the internet, which has  
24 certainly evolved but evolved more slowly, the wireless  
25 innovation is continuing really at a breathtaking pace.

1 It seems almost weekly there are new announcements in the  
2 paper followed by the product being introduced in stores  
3 by the end of that week or certainly next week.

4 So consumer expectations are driven by the  
5 capabilities of all these new devices and network  
6 features and applications, which continue to accelerate.

7 MS. HARRINGTON-MCBRIDE: Are cellphones or  
8 mobile devices generally more uniquely identifiable than  
9 someone's laptop or desktop computer?

10 Michael?

11 MR. ALTSCHUL: I'll take a crack at it.

12 MS. HARRINGTON-MCBRIDE: Sigh of relief amongst  
13 the rest of us. Thank you.

14 MR. ALTSCHUL: The answers are both yes and no.  
15 Every wireless device is going to have a unique  
16 identifier or a phone number or an electronic serial  
17 number that registers with the network. That is not a  
18 personal-identifying information. And, for those of you  
19 who are schooled in the Communications Act, a telephone  
20 number is not even considered to be part of CPNI under  
21 the Communications Act, but it does identify the device.

22 If you think about your own device or those in  
23 your family, the service provider, for the majority of  
24 devices, does not know who the user is. It's either a  
25 phone that comes from a family plan where the account

1 relationship will be with the mother or the father, then  
2 there will be additional phones for children and other  
3 members of an extended family. In that case, in the case  
4 of four or five devices under one family plan, the  
5 carrier is not going to be able to identify the phone  
6 number and device with a particular user.

7 Similarly, those of us who get phones from our  
8 employer on an enterprise basis, my carrier has no idea  
9 that my particular phone is assigned to me. They know  
10 it's assigned to CTIA.

11 So the code is a bit broken even though the  
12 device has a unique identifier.

13 MS. HARRINGTON-MCBRIDE: Alissa.

14 MS. COOPER: We have already had the two  
15 somewhat contrasting notions about how identifiable the  
16 device might be because, as Kristine pointed out, that  
17 mobile devices even when they are not attached to a name  
18 are quite personal. I think if we think about the  
19 service that Peter Eckersley mentioned this morning that  
20 EFF launched yesterday, the Panoptoclick, where you can  
21 use your browser and go and through the service find out  
22 how identifiable your browser is, I would be surprised if  
23 the same sort of logic doesn't apply to your phone. And  
24 that by using your phone or your mobile device just for a  
25 short amount of time, the pattern of behavior and the

1 data that gets resultingly stored on the device because  
2 you're the only one using it becomes actually highly  
3 unique to you. It just seems logical that if you are the  
4 one who is always using the phone, then that fingerprint  
5 of the phone really starts to become something that is  
6 unique and can identify you.

7 MS. HARRINGTON-MCBRIDE: I think that is a  
8 great beginning. I wanted to just sort of set the stage,  
9 just sort of set some of the distinguishing factors out.

10 And, with that, I think what we would like to  
11 do for the balance of the panel is to work from a  
12 hypothetical and Naomi will begin with that. And then we  
13 will ask you all some questions about that and try to get  
14 at some of the thornier issues relating to location and  
15 device size.

16 MS. LEFKOVITZ: Right. So we did not think we  
17 could really come to a law school and not come out with a  
18 hypo, so it would be particularly disappointing to the  
19 law students in the audience.

20 So today we have a little bit of a story about  
21 Agnus. Agnus is driving to a job interview. She is on  
22 the verge of being late. She uses her mobile to check on  
23 the traffic and sees that the way she was planning to go  
24 has traffic delays. So she takes another route and makes  
25 it to the interview on time.

1           It is mid morning by the time the interview is  
2           done. And just as she is thinking that she deserves a  
3           latte, the coupon service she signed up for sends Agnus a  
4           coupon for a nearby coffee shop.

5           After her coffee she wanders around the  
6           downtown area window-shopping. She comes across an  
7           interesting street performer and she uses her mobile to  
8           snap picture, which is automatically geotagged showing  
9           the latitude and longitude where it was taken, and  
10          uploads it to her social-networking page for her friends  
11          to see.

12          It so happens, though, that in the background  
13          of her picture is a man and a woman kissing. And, as it  
14          turns out, this man happens to be the husband of a friend  
15          of a friend, whom that friend believed was on a business  
16          trip. So, in fact, all is revealed when the wife  
17          browsing a social-networking site later that day notices  
18          the photo while visiting her friend's page.

19          But back to Agnus. It is now close to lunch  
20          time. And last night Agnus had made some big plans to  
21          meet up with friends. So she checks her friend-locator  
22          service to see who's around. She also opts to broadcast  
23          her hunger and her location to her Twitter account.

24          Giggling slightly, she reads a ping from  
25          someone who has a profile on her dating service that



1 noticed she was nearby. But then the service also sends  
2 her an ad for a nearby bar. And, ugh, she thinks, I may  
be joThced she was nearby. But thennearby bar. 2.D (1 )Tj 2.2404 -2.267tm



1           The 14-year-old one is 47 USC 222 from the  
2           Telecom Act of '96. And this classifies wireless-  
3           location information about your cellphone use as customer  
4           proprietary network information, CPNI. And so there is  
5           actually a bar on your telecom carrier disclosing that  
6           information without your consent except in emergency  
7           circumstances.

8           But a few caveats: It does not apply to  
9           aggregate information from which identifying features  
10          have been removed. And, most importantly for our  
11          purposes today, it only restricts telecommunications  
12          carriers. It does not restrict any of these other  
13          entities that we are talking about.

14          For broader restrictions you need to look to a  
15          law that was written when the primary focus of networking  
16          and computing was dialing into your BBS, and that's the  
17          Electronic Communications Privacy Act of 1986, which has  
18          been amended a few times in a few ways in a few ways, but  
19          primarily has the same structure it had 24 years ago.  
20          And that law restricts voluntary disclosures by a couple  
21          of different types of entities: Remote-computing  
22          services and electronic-communication service providers.

23          I will not belabor the point by reading the  
24          definitions, but suffice to say it is pretty clear your  
25          ISP and your phone company are electronic-communication

1 service providers. Moving beyond that, it is actually  
2 quite unclear what entities are covered by this law, and  
3 which is an ECS and which is an RCS, because there are  
4 differing rules for both and so it matters.

5 But this law not only regulates voluntary  
6 disclosures by the companies but also when the government  
7 can mandate disclosures from these companies, which is  
8 obviously our focus as civil libertarians as you might  
9 note from the "Come back with a warrant" sticker on my  
10 computer, but focusing on voluntary disclosures, whether  
11 or not a company needs your consent to disclose something  
12 depends on whether the information is communications  
13 content or noncontent information about your use of the  
14 communication service.

15 So in the typical scenario, that is the  
16 location information that your phone company has,  
17 reflecting your use of their phone or internet service,  
18 that is noncontent information and the company can  
19 disclose it without your consent. I think there are a  
20 few cases where your location information is indeed  
21 content, such as friend-finding services like Loopt where  
22 you are sending your location to other users of the  
23 service. And we are glad that Loopt and Google's  
24 Latitude have taken that position, which we agree with.  
25 But in many if not most cases the location information is

1 going to be considered noncontent at least by the carrier  
2 or the service provider such that it could be disclosed  
3 without even your knowledge or consent.

4 And so the current statutory regimes are really  
5 quite underprepared in dealing with this proliferation of  
6 services that have your data. You know not only is it  
7 weakly protecting the data even to the extent the law  
8 applies at all, in many cases the law won't apply at all  
9 because the service doesn't qualify as an electronic-  
10 communication service provider or a remote-computing  
11 service.

12 So if you are looking to the federal statutes  
13 to help you, it is not looking very good.

14 MS. LEFKOVITZ: Darren, do you want to speak?

15 MR. BOWIE: So in addition to the statutes that  
16 Kevin mentioned, I would point out a statute that now is  
17 nearly a hundred years old, and that's the Federal Trade  
18 Commission Act. And we should certainly point out that  
19 that statute has a very important role to play in this  
20 hypothetical, in addition to all of the state deceptive-  
21 practices statutes modeled on the FTC Act.

22 So a number of the parties in this hypothetical  
23 are subject to FTC jurisdiction. So all of the third-  
24 party application providers here, the dating service, the  
25 coffee-shop coupon service, all of those are subject to

1 the FTC Act. And they have a duty, of course, to  
2 disclose all the material terms and conditions of their  
3 service, including are they receiving and using GPS  
4 information, how are they using that information, are  
5 they going to be sharing that with advertising networks,  
6 with advertisers. And I think about this issue about the  
7 ad for the bar that the person received.

8 So it is important to realize the important  
9 role and the flexibility of the FTC Act when we look at  
10 this hypothetical, in addition to the statutes that Kevin  
11 mentioned.

12 MS. LEFKOVITZ: Alissa.

13 MS. COOPER: Just to go back for one second to  
14 the CPNI rules, we have talked a bit today about the Fair  
15 Information Practices. I just wanted to reenforce the  
16 point that not only do the CPNI rules only apply to the  
17 carriers, but whether you think the FIPs are broken or  
18 you think we have not done enough to address all of the  
19 FIPs, the CPNI rules don't come close to addressing the  
20 full set of Fair Information Practices. They are really  
21 only about disclosure and sort of nominally about  
22 consent. So there is nothing in there about security or  
23 access or minimization or any of the other Fair  
24 Information Practices.

25 MR. BANKSTON: I will add a clarifying note

1 building on that. The ECPA -- Stored Communications Act  
2 portion of the ECPA and the CPNI rules do not restrict  
3 use or retention in any way. It is all about disclosure,  
4 so.

5 MS. COOPER: One other note on the  
6 hypothetical. I think we tend to think with the  
7 proliferation of smartphones and all the app stores that  
8 are out there, we think a lot about these cool new apps  
9 that everyone has on their mobile phones and, in  
10 particular, location-based apps. I just wanted to draw  
11 people's attention to the fact that it is not only apps  
12 developed for specific platforms that can gain access to  
13 the mobile device and to things like location  
14 information, but it is also Websites.

15 Last summer there was actually a draft standard  
16 put forward that would standardize the way that Websites  
17 can ask Web browsers for your location information. And  
18 all of the major mobile browser platforms have  
19 implemented it.

20 And what this means is that, as opposed to the  
21 scenario that we have been used to and that Darren  
22 mentioned at the top about having to develop applications  
23 differently for each kind of platform, what the Web did  
24 for desktop computing it also has the potential to do for  
25 mobile computing. And what that means is that we have

1 the potential to see many, many, many more Websites that  
2 can gain access to the mobile, gain access to location  
3 information much more easily because they can be  
4 developed just one time for the Web.

5 So some of those apps that Agnus may have used  
6 in the hypothetical, they do not necessarily need to be  
7 purpose-built for one device. They could be built one  
8 time for the Web and used on any device.

9 MR. BOWIE: One other thought too, we are  
10 talking about the laws that apply, but of course there  
11 are significant self-regulatory initiatives that apply as  
12 well. So, for example, and Mike can certainly speak to  
13 this, CTIA has issued location-based services guidelines.  
14 To the extent the actors and providers in this  
15 hypothetical are members of CTIA, they are bound by those  
16 guidelines. Also the MMA has guidelines that would apply  
17 as well.

18 So I think it is important to consider those  
19 guidelines. We can talk about how effective they are,  
20 but they are relevant to the situation.

21 MR. ALTSCHUL: That is actually why I had  
22 raised my tent. I think there has been for some time a  
23 recognition that the statutes do not reach where the  
24 technology and the applications are today. And a little  
25 history might be helpful.



1           The CPNI rules were passed as part of the '96  
2           Telecom Act, but there was no reference to location as  
3           proprietary information until 1999 when an amendment  
4           sponsored by Congressman Markey was passed. And that was  
5           because the FCC in about this timeframe had mandated that  
6           wireless carriers provide location information in  
7           connection with 911 calls.

8           As a result of wireless networks gaining the  
9           capability to actually identify a user's location on a  
10          much more granular basis than was possible before,  
11          Congress amended the statute with carriers and the kind  
12          of technology that was being contemplated more than ten  
13          years ago in mind.

14          As we already discussed on this panel,  
15          increasingly the carrier is not going to be involved with  
16          either determining the user's location or even in  
17          transmitting it to the application. Most of us or many  
18          of us who now have smartphones, I started to say "many,"  
19          it is not going to be long before it is a majority of  
20          users, wifi is built in to the devices as an alternate  
21          transmission path. Depending on the operating system,  
22          the phone will default to the wifi network before the  
23          wireless carrier's network, at which point the user will  
24          never know which air interface is being used, but the  
25          location information and instructions to the application

1 will be sent without ever touching the carrier's network.

2 Two years ago when CTIA started its best  
3 practices for location-based services, based on the Fair  
4 Information Practices of the Federal Trade Commission, we  
5 had assumed that carriers would be central to the  
6 determination and transmission of the user's location.  
7 We have just gone back and are in the process of revising  
8 the scope of our guidelines and best practices to  
9 recognize the fact that in two years the world has  
10 changed and increasingly devices and applications are not  
11 just agnostic to the network but oftentimes independent  
12 of them.

13 MS. LEFKOVITZ: A quick last word.

14 MS. van DILLEN: Yes. Darren also mentioned  
15 the Mobile Marketing Association Global Code of Conduct  
16 and I just wanted to highlight the pieces of that which  
17 include the notice and the choice and consent,  
18 customization and constraint, security and then  
19 enforcement and accountability. And those are the  
20 expectations that the Mobile Marketing Association has  
21 for mobile marketers.

22 MS. HARRINGTON-MCBRIDE: So obviously this is a  
23 very complex ecosystem, to use an overused word yet  
24 again. And there are a lot of factors at play. I think  
25 one of the things that we really wanted to hone in here

1 on is elucidate for us some of the underlying concerns  
2 about access to locational data. Because, obviously I'm  
3 with Kevin, I would be at the water cooler doing my Yoga  
4 breathing if this were my exam time. It's a very  
5 complicated hypothetical, there are a lot of people in  
6 play, there would be a lot of analysis that needs to be  
7 done, and obviously we only have 40 minutes or so  
8 remaining, so let's talk about at a high level. What are  
9 some of the location-privacy concerns and then how do  
10 they play out differently depending on who is obtaining  
11 that location information and how responsible those  
12 parties are?

13 So who would like to tackle that one?

14 Amina.

15 MS. FAZLULLAH: I am going to talk about some  
16 of the harms, but I guess briefly I think when you  
17 realize that people know your location, I think there are  
18 a few things that can start to come up. If an employer,  
19 so if an employer is resource tracking, like using a  
20 mobile phone to know where their bus drivers are, where  
21 their crossing guards are, where other employees are, if  
22 they don't give the employee the ability to have some  
23 kind of privacy control, then they now have information  
24 on what the employee is doing even on break, perhaps even  
25 after hours. So there can be employment issues related

1 to that, employee-privacy issues related to that.  
2 I think that especially with healthcare there  
3 is also some issues. If information about kind of where  
4 you are spending a lot of your time, if you are going to  
5 -- it can be identified that you are spending a lot of  
6 time in a hospital, a doctor's office, or some other  
7 location that can give people an idea of what your  
8 healthcare situation is like, that can have some kind of  
9 effect down the road in terms of access to insurance, or  
10 just depending on how that information is distributed,  
11 how granular it is, what is said about it, who else is  
12 having it, that all can affect your opportunities for  
13 services down the road. I mean that is just picking one  
14 particular piece of information.

15 Then there is also sort of identifying people  
16 that maybe you don't want to know anymore. So worrying  
17 about domestic violence issues and whether or not  
18 somebody will now have access to your location, say,  
19 through social networking, through friends of friends.  
20 Kind of going back to the hypothetical, there are some  
21 issues related to that where you can clearly see if

partiiuted,



1        need to think about it a little bit specifically. I mean  
2        for a minute there I freaked out because I realized  
3        everybody here knows where I am and they know my  
4        location. Kevin's here and I knew he would protect me,  
5        but I think there are a few situations where it matters,  
6        right.

7                So domestic violence and safety I think is  
8        something -- it is sort of another path, and we have done  
9        a lot of work in that area. I think it is a little  
10       outside the scope of this discussion, but I think with  
11       regard to employers having access, government having  
12       access over long periods of location-history information,  
13       I think that is a sensitive situation. We are involved  
14       in the ECPA reform that both CTD and the EFF are  
15       participating in and pushing really hard.

16               We are concerned about passing complex -- you  
17       know this is a complex situation, so to pass more  
18       complex, outdated laws to replace current, complex,



1 MS. HARRINGTON-MCBRIDE: About a year is our  
2 typical retention period.

3 MR. KNAPP: Okay. Is that on your Website?

4 MS. HARRINGTON-MCBRIDE: I got to tell you, we  
5 are doing this through Berkeley, so you have to check  
6 their terms of service.

7 MR. KNAPP: Okay.

8 MS. HARRINGTON-MCBRIDE: But I wonder if you  
9 would feel differently --

10 (Laughter.)

11 MR. KNAPP: So you guys are a third party in  
12 this? Oh, this is -- is that okay?

13 MS. HARRINGTON-MCBRIDE: So your point is well  
14 taken, that you are here and everybody knows you are  
15 here, but would you feel differently if Kevin were to  
16 follow you around for a year and then publicize your  
17 whereabouts? So how about retention of data? That is  
18 something your company has dealt with in a particular  
19 way. Can you tell us how you have done that?

20 MR. KNAPP: Sure. So we tend to look to the  
21 user, right, so we try to get out of a legalistic sort of  
22 framework and mindset with this stuff and say, okay, what  
23 do we need to drive our business and what does the user  
24 want us to do, sort of, on their behalf. And we think  
25 those are the important areas to look at it.



1           So we do think location is the kind of thing  
2           that is less sensitive on a one-off basis and more  
3           sensitive over time. So we had to provide our basic  
4           friend-finding service need to have a location fixed at a  
5           given period of time, right, to show where you are, based  
6           on your settings and what you have opted into, et cetera.

7           But otherwise to provide that basic friend-  
8           finding service need, we do not need to keep that

1 service.

2           And it is interesting because there is a bit of  
3 a tension, and we talked a little bit about safety. In  
4 Amina's examples there is a tension between law  
5 enforcement and what sometimes the government asks you to  
6 do with regard to retention and what the privacy side of  
7 it is. And so we also -- and again thank you to the EFF  
8 and CDT has sort of helped us figure out some strong  
9 policies around that with regard to not only our  
10 retention but what the legal requirement is for access to  
11 that information.

12           And we have taken a position I think that

reflects where we all want to ar isnd w oase3 bytRposition I taro tarelbTD D (7 )Tj6rir0 T6mrm Al ( p A

1 planning clinic, go to that cancer specialist, attend  
2 that secret union meeting, attend that controversial  
3 political or religious gathering with some freedom and  
4 anonymity.

5 Now there are records that can reveal those  
6 things. And, to a great extent, the collection of that  
7 information and the handling of that information is  
8 unknown to the person carrying the phone or other mobile  
9 device.

10 And I also think it is important to note that  
11 just as we were talking about in the social-networks  
12 panel, there are front-end and back-end issues. There  
13 are the back-end issues of who is collecting what and how  
14 long are they keeping it and what are they using it for,  
15 but there are also the front-end issues of how are you  
16 managing the sharing of that information with your  
17 friends and are you inadvertently disclosing more about  
18 your location to your friends than you actually intend.  
19 Are you going to accidentally allow your employer to find  
20 out that you went to that secret union meeting or your  
21 wife to find out that you went to that iffy bookstore.

22 And so there are several levels here and it is  
23 not similar to the social-networking issue.

24 MS. HARRINGTON-MCBRIDE: Alissa.

25 MS. COOPER: One other property of location

1 information which I think makes it special that has not  
2 been mentioned yet, and I usually use myself for this  
3 example but I will use Brian since he is the privacy  
4 fundamentalist on the panel.

5 There is only one person who spends his daytime  
6 hours at Loopt and his nighttime hours at Brian's house,  
7 assuming that your wife does not work at Loopt and your  
8 dog does not have a cellphone, and that is Brian.

9 (Laughter.)

10 MS. COOPER: And that is Brian, he is the only  
11 person. And so it does not take very many days of  
12 collecting that location information from Brian's device  
13 to figure out that it is him, not knowing anything else  
14 really other than having a phone book, basically.

15 I think that -- it's something that is special  
16 about location. It is the reason why some companies that  
17 collect location information have done things, like cut  
18 off the two ends of every trip that they collect so that  
19 if you are using navigation directions, Google, for  
20 example, does this with their traffic data, they will  
21 snip off the ends of each trip because -- and kind of  
22 randomize it -- because those two ends can be used to  
23 identify you. It is another reason why retention is so  
24 important, because if you retain that pattern over just a  
25 small number of days, you can start to identify someone.

1           So it is not the case that it needs to be  
2           married to an identity. In and of itself, the behavioral  
3           movements tied with location can identify a person.

4           MR. KNAPP: I am going to jump right in. So I  
5           think that's right, but I think just to use those two  
6           examples, gazillions of people know where I work and a  
7           lot of people know where I live to, especially a lot of  
8           direct-marketers have my location, have my home address.  
9           All my neighbors, a number of folks who have been over  
10          for dinner parties. And so those two locations are not a  
11          secret for me at least and I have not made an effort to  
12          keep them private from folks.

13          So to the extent that Alissa is talking about  
14          using those locations to then identify me as a person,  
15          reverse-engineer and use some other -- tie that to other  
16          information and things I am doing on my mobile device, I

1 particular locations and, yes, I am usually at home at  
2 night and I am usually at Loopt during the day, are just  
3 not a big secret, right? And that is my point around  
4 being really specific about when location becomes  
5 sensitive and in what context and vis-a-vis what kind of  
6 parties.

7 MR. ALTSCHUL: To follow up around the dialogue  
8 between Brian and Alissa, certainly some, probably the  
9 overwhelming majority of location information is not  
10 going to be troubling to the user, but there will always  
11 be a category of information which the user would not  
12 want shared. And that gets us back to the notice and  
13 consent and the control principles that are central to  
14 all of the privacy discussions.

15 And going back to our now-forgotten law school  
16 hypothetical, each of the different applications  
17 indicates how the user has had to opt in to a particular  
18 application, whether it is realtime traffic and GPS  
19 navigation or uploading to a social network and posting  
20 on Twitter a photograph, a lot of settings have to be  
21 enabled by the user, not just the click through for the  
22 scrolling of the consents but the phones need to be  
23 provisions, software needs to be downloaded, there are  
24 choices as to how the information is to be displayed,  
25 what kind of information you get back. And it is sort of

1 common-sensical that the more the user has to interact  
2 with the application, the better understanding and better  
3 control the user is going to have of that information.

4 Just as an aside, my favorite part of the  
5 hypothetical, of course I think we all recognize, was the  
6 photography on the street being uploaded. This is a plot  
7 from an opera, actually. It would be a very, very good  
8 plot for maybe the first new opera of the twenty-first  
9 century.

10 MS. LEFKOVITZ: Well, that is a really good  
11 segue on the issue of notice, so we are all very  
12 interested in what kind of experimentation is going on in  
13 this space with respect to notice. Is there any research  
14 or feedback on how consumers are viewing this?

15 Brian, do you want to...

16 MR. KNAPP: I think the top Web and mobile  
17 companies out there are some of the best around in terms  
18 of handling this stuff. So I think Apple, for example,  
19 the location-based applications, it is hardcoded into the  
20 OS to provide a quick, translucent notice to let them  
21 know that an application has accessed the location API in  
22 the iPhone.

23 So it is informative, but it also does not  
24 create a lot of friction between the user and the  
25 application that the user does not want. I think other

1 OEMs and manufacturers are doing that as well, so I think  
2 Google and Android are doing a nice job in that regard  
3 and Rim with BlackBerries as well.

4 I do think the mobile environment need to be  
5 particularly in tuned to the size of your notices, if you  
6 want to come across to the user and have them understand  
7 sort of what they are participating in. And, again, I  
8 think that is why it is best to look at it from sort of a  
9 customer-service and product-development and a privacy-  
10 by-design perspective versus sort of trying to check some  
11 legal box.

12 We do not believe opt in is some sort of  
13 magical silver bullet and we get concerned when people  
14 throw it around that way, but we do believe that users  
15 should have a sense of what an application is going to do  
16 when they open it and to the extent notice is  
17 appropriate.

18 I do think that there is an expectation and  
19 there is going to be an expectation by users that these  
20 smartphones can locate themselves. Often it is put,  
21 especially sometimes in surveys and such, where they will  
22 ask, 'Well, you know if such-and-such was tracking you  
23 all the time, how would you feel abtj -2tt thw1.z0l bet  
24 if you asked it a different way and said to the user, 'Do  
25 you expect your \$400 smartphone to be able to locate





1 E911 service without them having to do anything like  
2 special, I think people would sort of break down in two  
3 different packs.

4 I think if you wanted to have maybe some  
5 security measures so if your phone is stolen that you can  
6 identify it or if you are doing some kind of product  
7 location, if you have like a car that's stolen, you want  
8 to identify it, this is a little off the map, but again  
9 people would take that differently.

10 So I think it breaks down to use: How is it  
11 being used and who is using it. And so that is when  
12 locational information actually -- that is when notice  
13 and consent start to really come in because they are just  
14 expectations from your service provider, what you expect  
15 them to be able to do and why they would need to know  
16 that information. And then there are expectations from  
17 the other commercial applications that you are using and  
18 why they would need that information and who they are  
19 sharing it with and what it is being used for.

20 MS. COOPER: I think notice in the form of the  
21 screen that pops up to ask you if it is okay to share  
22 your location in this instance is one aspect of  
23 transparency and involving the user in the  
24 decisionmaking, but it is really only one small aspect.

25 And I agree with what Brian said, that many of

1 the platform providers have done a good job with the  
2 upfront consent. So when you go to a location-enabled  
3 Website, when you use a location-based application it  
4 will ask you if this is really what you want. But it  
5 does not stop there and many of the platforms seem to  
6 think that it does.

7         So if you want to see a list of all the  
8 applications that you have given your location to, if you  
9 want to be able to create a white list or a black list so  
10 that you don't have to go through the opt-in process  
11 every time or so that some sites or some applications can  
12 just never have access to your location, if you want to  
13 get a reminder every now and again of which sites or  
14 which services you have given your location to, I know  
15 that is a feature that Loopt includes but it is not a  
16 feature that every platform and every application

1 can assume that there are some situations where our  
2 consumer seems to be surprised and not have expected when  
3 her information has been shared.

4 I think, again, we have to come back to what  
5 does a reasonable consumer expect about how their  
6 information is going to be used. I think they do expect  
7 that information will be shared with their carrier for  
8 certain technical-related reasons, but here she did not  
9 seem to expect that she would be getting an ad from a  
10 bar. So I think it is useful to look at what disclosure  
11 was made to her and how that should have been made.

12 So privacy settings are very important and I  
13 absolutely agree there is a lot of work to be done in  
14 this area to bake privacy settings into the device and  
15 through platforms. But, as we do that, we have to focus  
16 on where is the harm to the consumer and what are their  
17 expectations, and this hypo is an example of that.

18 MR. BANKSTON: Yes. My iPhone is saying Google  
19 Maps wants my location. That is one type of notice, but  
20 it is not notice at all in terms of how long Google  
21 stores that data, whether and what steps it takes to  
22 deidentify it, et cetera, et cetera. Something that  
23 Google has not made public.

24 And you know we had people like Facebook and  
25 Google coming up and saying, we are the good guys and we

1 are here to talk to you about what we do and be upfront.  
2 And even they, we do not really know exactly what they  
3 do.

4 You bring it closer to home and people do not  
5 even know what records their carriers are storing. Again  
6 I like to think I am an expert in this area, I have seen  
7 a handful of exemplars of what types of cell site records  
8 companies keep, but I do not know what the standard  
9 practice is, how long they keep it, whether they  
10 deidentify it.

11 So I think there is a real serious problem in  
12 terms of consumer knowledge or regulator knowledge about  
13 exactly what is being collected by whom and what they are  
14 doing with it. We do not have all the answers we really  
15 need to those questions. In fact, not only is about  
16 notice about use or disclosure or use, also disclosure  
17 about capabilities.

18 For example, even if you do not use any GPS-  
19 based location-based services your carrier can still  
20 obtain your GPS location, as was most recently  
21 established when Sprint announced at a surveillance  
22 conference, described the interface they have set up for  
23 law enforcement to go and obtain your GPS location  
24 without your knowledge.

25 So I do not believe notice and consent is a

1 silver bullet. I also think, though, however, that  
2 notice is incredibly important and people are not getting  
3 notified enough of what is going on.

4 MS. HARRINGTON-MCBRIDE: Notice -- oh, Amina.

5 MS. FAZLULLAH: I just wanted to add one more  
6 point, is that with notice comes control. So I think  
7 what is maybe a positive benefit to marketers or  
8 applications providers, when you send them an ad for a  
9 bar that they do not want, if they are able to say, hey,  
10 you got it wrong and here is what is right, because they  
11 actually want to get the right stuff, you provide a  
12 platform where the consumer can now trust you and have a  
13 relationship with you and correct things when you get it  
14 wrong because they actually want to get stuff that's  
15 right. I think that would be really hopeful for the  
16 industry and it would grow control for consumers and they  
17 would actually be able to understand, actually  
18 participate in the process of giving their information  
19 and getting something back for it.

20 MS. HARRINGTON-MCBRIDE: Okay. Kristine, -- I  
21 would love to have --

22 MR. ALTSCHUL: If I could follow up, since  
23 Sprint is not here to defend their honor, I think we have  
24 all agreed that the scope of what access law enforcement  
25 has or civil subpoenas have to this information is beyond

1 our scope, but in the example Kevin gave it actually was  
2 an example of law enforcement pursuant to a warrant --

3 MR. BANKSTON: I didn't say it was pursuant to  
4 a warrant.

5 MR. ALTSCHUL: Well, law enforcement gained the  
6 -- every time you receive a warrant --

7 MR. BANKSTON: For legal process.

8 MR. ALTSCHUL: For legal process. Every time  
9 you receive one, just as -- let me -- have it on the back  
10 of it -- the service provider is prohibited from  
11 providing notice --

12 MR. BANKSTON: Well, that --

13 MR. ALTSCHUL: -- so that I just want to -- I  
14 know you did not intend to be misleading, but for those  
15 in the audience who are not familiar with the particular  
16 context of Sprint's statement at a conference on this,  
17 they should know that in that particular example Sprint,  
18 pursuant to the process they received from the  
19 government, could not give notice to the customer.

20 MR. BANKSTON: To clarify what I was  
21 criticizing, I was criticizing the fact that consumers do  
22 not understand that their GPS can be remotely turned on  
23 and accessed by the carrier, not that the government can  
24 use legal process to secretly do so. It was a fact about  
25 people not understanding the technical capabilities that

1 exist, so.

2 MS. HARRINGTON-MCBRIDE: Okay. So, Kristine, I  
3 would like to talk to you a little bit about advertising  
4 in the mobile space. Obviously location by some accounts  
5 from marketers is the holy grail. It is the thing that  
6 everybody wants. Because if you know where people are,  
7 you have some context, you have their information about  
8 what they are close to, and you can probably very readily  
9 monetize an advertising structure.

10 So I want to get to that because we only have  
11 about 15 minutes left, so tell us a little bit about your  
12 perspective on the things that we have talked about about  
13 notice that may impact advertising. So, for example, a  
14 consumer may opt in to a service and know full well that  
15 they are using it for their own purposes to, for example,  
16 find out where their friends are in a given space or to  
17 get directions to something.

18 To what extent are consumers aware that  
19 advertising is part of that business model and then to  
20 what extent do they have control, as Amina suggested,  
21 over what advertising they see?

22 MS. van DILLEN: Right. Well, we see that  
23 location-based advertised is many more times valuable  
24 than regular advertising, so that is many multipliers.  
25 And our recommendation is is that you give customers



1 consideration for when they provide you with information  
2 as an advertiser, which means that if a customer is  
3 providing their location to get information about what is  
4 around their location, they would reasonably expect that  
5 that location is then being shared to provide advertising  
6 back.

7 We find that consumers are familiar with that  
8 behavior online, they expect that advertising is going to  
9 supplement the data that they are receiving for free, and  
10 so I think it is very important to note that it is that  
11 consideration, it is: I am a consumer, I'm supplying you  
12 with my personal information because in turn you are  
13 giving me information that I am looking for for free.

14 MS. HARRINGTON-McBRIDE: Sounds like it may be  
15 akin to the online model.

16 Ms. van DILLEN: Yes, and we find that the  
17 consumers are comfortable with that, that that's what  
18 they expect.

19 MS. HARRINGTON-McBRIDE: And so does that  
20 expectation -- to what extent do you think then, for  
21 example, consumers would understand behavioral  
22 advertising in the mobile context? And to what extent is  
23 behavioral advertising combining, for example, that  
24 locational piece into a broader profile of a consumer and  
25 their interests and habits, how is that data being



1 I mean how does a user know how to manage their privacy?  
2 Do they have to go into their device settings, their OS  
3 settings, their carrier-privacy policies, their  
4 application?

5 Ms. van DILLEN: I do not think it is that  
6 complex right now. I think in a lot of cases it is  
7 setting up an application and it is selecting the  
8 different types of brands you want to be engaging with.  
9 I think because that provides a value for the consumer  
10 and for the brand, that that's one of the first setting  
11 features the consumer comes across when they select that  
12 application. The way I have seen it set up on the banner  
13 ads, it is a menu icon on the side and it is something  
14 that the consumer clicks for more information, and there  
15 are a list of things and they can opt out in that way.

16 And then for text messaging there is always an  
17 option to stop text messaging. And we are very clear  
18 about the guidelines for doing that, making sure the  
19 consumer understands that they can always press stop to  
20 stop text messaging alerts.

21 MS. HARRINGTON-McBRIDE: What role does  
22 government regulation have to play in this space going  
23 forward? We have got about ten minutes left, so let's  
24 think about the self-regulatory standards to some extent  
25 are in place. I know Mobile Marketing Association is

1 still looking at finalizing location-based service  
2 regulations.

3 Michael has told us that CTIA is revising and  
4 trying to take account of some of the rapid changes that  
5 have taken place.

6 So what are the standards that should be set,  
7 whether they are set by a government agency, a self-  
8 regulatory body, what should be the baseline code of  
9 conduct for behaving responsibly in this area?

10 MR. BOWIE: So I can start with that, and there  
11 are some important self-regulatory initiatives already in  
12 place, and we have discussed those. I think there needs  
13 to be further work done on refining some of those  
14 initiatives to the unique issues involved in the mobile  
15 ecosystem.

16 So there has been a lot of discussion about  
17 behavioral advertising. Are there specific aspects of  
18 mobile behavioral advertising that need to be addressed,  
19 certain different types of disclosures or other ways to  
20 do that. So that is work that should continue.

21 When we get into the question of government  
22 regulation in this area, I think before we get to that  
23 there are two things that the Commission, to take an  
24 example, could do now before we consider whether  
25 additional regulation is necessary.

1           One, I think there is a very important role in  
2           consumer and business education, and the Commission has  
3           done an outstanding job in other areas. In the last  
4           decade, the Commission produced a very important  
5           education piece called Dot Com Disclosures, on how to  
6           make disclosures in the online environment. I still have  
7           my very old dog-eared copy that I actually still use.

8           I think something targeted to mobile  
9           disclosures and with examples and when a just-in-time  
10          notice might be appropriate, I think that would be very  
11          important and something the Commission could do now while  
12          we think about these big questions about regulations.

13          Also I think there is a role for increased  
14          enforcement in this area, so the Commission has done an  
15          outstanding job in privacy enforcement, I think some  
16          enforcement targeted in the mobile space also would be  
17          useful to send a message that this is an important area  
18          that's a priority. I think it is fair to assume that  
19          there are bad actors involved here who are using  
20          information without proper disclosure and consent, in  
21          nefarious ways. So some increased enforcement by the  
22          Commission also would be important.

23          And the state should also be engaged. I wanted  
24          to make that point as well, the state AGs should be  
25          involved in these discussions. They are going to become

1 involved in enforcement, so it is important to include  
2 them as well.

3 When we move to the question of regulation, I  
4 do think this is an area, because there is so much  
5 innovation, there is so much change, as Mike pointed out,  
6 the mobile world really has changed almost completely  
7 within the past couple of years, to me it would be  
8 difficult at this stage to come up with regulations,  
9 given all the changes, and the opportunities I just  
10 identified to take action in this area already under  
11 Section 5 and existing law.

12 MS. COOPER: So I am really glad that Darren  
13 brought up enforcement because otherwise our panel would  
14 have been the only one to not suggest that our friends at  
15 the FTC engage in more enforcement, and I think he is  
16 absolutely right that this is an area that is ripe for  
17 further investigation. And I think there are bad actors  
18 out there that within the FTC's -- even under the harm's-  
19 based standard that has sort of dominated the paradigm of  
20 late, I think you could find instances where unfair and  
21 deceptive practices are going on.

22 But to point out some of the examples that  
23 Amina and Kevin brought up, I think if you think more  
24 broadly about the dignity-based standards that Director  
25 Vladeck has spoken about in recent months, I think there

1 is an even broader base and potential for further  
2 enforcement.

3 One other aspect of some existing FTC authority  
4 links in tightly with the self-regulatory programs that  
5 already exist. And I kind of wonder about how those  
6 programs are enforced and what the kind of accountability  
7 and compliance mechanisms there are to back up those  
8 self-regulatory programs, because without that kind of  
9 teeth, it is not really clear whether -- if no companies  
10 are getting kicked out of the self-regulatory program or  
11 if there is actually no compliance measures that are  
12 brought to bear, then it is unclear whether the self-  
13 regulation is really actually working.

14 I think as far as further regulation and  
15 legislation goes, obviously CDT is highly in favor of  
16 baseline federal privacy legislation and we think that  
17 location information could be part of that framework  
18 where we think about sensitive kinds of information. I  
19 think location information and perhaps other mobile-  
20 device data could be incorporated into that kind of  
21 framework.

22 And, as we've spoken about earlier, ECPA and  
23 ECPA reform is another area where new legislation is  
24 absolutely warranted to level the standard and make sure  
25 that when we do get requests from the government for

1 location information, that the probable-cause warrant is  
2 the standard that is in use.

3 MS. HARRINGTON-McBRIDE: Amina.

4 MS. FAZLULLAH: I think I don't want to sound  
5 like I am just saying ditto, but I think that are three  
6 ways that we can -- if we can strengthen user control, if  
7 we can strengthen sort of rules around requiring  
8 transparency when someone starts to engage with a company  
9 that is going to ask for this information, and then of  
10 course compliance and enforcement.

11 So I think what is difficult is that while  
self-regulation is probably the first place where you are



1 problems online and in the mobile space.

2 MS. HARRINGTON-McBRIDE: Michael, would you  
3 like the last word on this part?

4 MR. ALTSCHUL: I don't know if I will get the  
5 last word, but I would like it. One thing that we all  
6 need to do a better job at, and the -- see, already  
7 (referring to Mr. Bankston's table tent) -- and the  
8 Commission needs to be congratulated for these dialogues,  
9 is education. It is part of the Fair Information  
10 Practices and it is something that I know in our  
11 association we have recognized the need that we all need  
12 to do a better job of educating consumers, particularly  
13 with technology and applications that are evolving and  
14 changing so quickly beyond what expectations of even last  
15 year would have been.

16 Secondly, I am in the camp that the Federal  
17 Trade Commission Act does provide enforcement authority.  
18 And if the Commission's guidelines -- for example the  
19 behavioral advertising guidelines were incredibly  
20 welcomed by our industry, an awful lot of activity had  
21 been held back waiting for some guidelines, sort of rules  
22 of the road that would allow various ventures to proceed.  
23 So more of those. They can be revised, they can be less  
24 formal than statutes.

25 And if there is to be an updating of statutes,

1 obviously Congress is always aware of the fact that they  
2 try to future proof their rules. Unfortunately they're  
3 rarely successful in an industry that's as dynamic as our  
4 industry and the computer industry. So there is always a  
5 risk when Congress is in session.

6 The one thing that we would not endorse is a  
7 system of 50 different state sets of privacy rules,  
8 particularly for a mobile technology and Web-based  
9 technology. It becomes a patchwork quilt for educating  
10 consumers, it becomes a nightmare for not just carriers  
11 but for customers who operate in a lot of jurisdictions.  
12 The best example of course is those of us who live in the  
13 Washington, D.C. market where there are three  
14 jurisdictions, all one bridge across -- there is one  
15 bridge that is in three different jurisdictions. But  
16 with that, if there is to be rewriting and privacy laws,  
17 it should be at the federal level with future proofing in  
18 mind.

19 MS. HARRINGTON-McBRIDE: Thank you.

20 MS. LEFKOVITZ: Okay. Hang on, Kevin, I have a  
21 question for you. So what are some -- are there any  
22 other ways to mitigate privacy risks in mobile computing?

23 MR. BANKSTON: That is what I was going to talk  
24 about. I do not want to ditto or take issue with  
25 anything said on the regulatory scheme -- regulatory



1       there can be competitive or other political or other  
2       benefits for companies to look into these kinds of  
3       approaches.

4               So if you want to look at that paper just  
5       Google for EFF on locational privacy, or Bing or Ixquick  
6       or whatever search engine you prefer.

7               MS. COOPER: I would just add that we also  
8       should not lose sight of all the privacy protections that  
9       exist for other forms of data. They also work for this  
10       kind of data as well. And if you think about in a  
11       security context there are some Web browsers that  
12       communicate with location services, the service that  
13       actually locates the device. Firefox is one of them that  
14       communicates with its location provider over an encrypted  
15       channel. There are some that do not.

16               We have known for a long time that encrypting  
17       the communications channel is one way to prevent  
18       eavesdropping and help protect privacy. And yet it is  
19       kind of a baseline protection that hasn't really become  
20       ubiquitous in the marketplace. So I think there are new  
21       techniques that can be very useful. There are also very  
22       old techniques that would also help out.

23               MS. HARRINGTON-McBRIDE: Brian -- oh, hang on a  
24       minute. I am going to ask Brian a quick question here  
25       because, Brian, you are the guy in the business here, so

1 let's talk to you for a minute about these potential  
2 technological solutions, cryptography, something that you  
3 think would be workable in a business context, is it  
4 scalable?

5 MR. KNAPP: I think there are some questions  
6 about that. I mean I think it sounds great. So, first  
7 of all, just to step back for a second, I do not know  
8 that some of this stuff is not already in place. So on  
9 the iPhone an application can know only your UDID, which  
10 is not tied to you. And you can hit their location, the  
11 API, to get a location fix. Combine that with the UDID,  
12 and you have exactly nothing in terms of who the person  
13 is, and you can provide a very robust location service.

14 BlackBerries has a similar approach, actually.

14 I mean there is a device I.D., but if you kt if you kt if yo6f

1 coincidence that most of us are taking privacy and data  
2 security pretty seriously.

3 So we are looking to implement a strong data-  
4 security measure balanced with what is practical. I mean  
5 the way the Kevin put it, that it would cost the provider  
6 a little bit more to do x, y, and z, well, what he is  
7 really saying is it is going to cost the user more. And  
8 so to the extent users are looking for advanced  
9 technologies to keep them private, then of course they  
10 are welcome to pay for that kind of stuff. But it is not  
11 necessarily our experience that users are willing to pay  
12 a lot more to go out of their way when some of these  
13 technologies are already in place.

14 MS. HARRINGTON-McBRIDE: Amina.

15 MS. FAZLULLAH: I guess I just wanted to add  
16 that at least on the mobile platform there is not -- when  
17 you go in the online world and using your computer, there  
18 is a lot of stuff that users can do to check who has been  
19 following them or, to some extent, to look at cookies or  
20 look at other things. And on your phone it is very  
21 difficult to be able to do that, even though you are  
22 starting to go online or you are being behaviorally  
23 targeted or tracked for ads.

24 And so since you do not -- again this is going  
25 back to user control, but actually I am more talking to

1 the companies that are sitting up here, it is another way  
2 again to build trust with your customer. If you actually  
3 build in -- if Motorola has a device or if Sprint decides  
4 to allow consumers to be able to access this information  
5 and clear it out or control it, then you will have a lot  
6 more awareness and understanding and smarter consumers  
7 who are going to be just happier consumers generally.  
8 And it is another easy way of generating trust and

1 PANEL 5: TECHNOLOGY AND POLICY

2 MS. RICH: So welcome to Panel 5, Technology  
3 and Policy. I am Jessica Rich. My Comoderators are  
4 Katie Ratté and Naomi Lefkovitz, who I think I just hit,  
5 who I think are going to let me do most of the talking  
6 and rest on their laurels from earlier in the day.

7 Our topic for this panel is Technology and  
8 Policy. We are going to build on other panels and take  
9 it the next step, which what are the implications of the  
10 issues we have discussed for policy and for policymakers.

11 So I have a great panel to help me discuss  
12 these issues:

13 Ellen Blackler, right here, is Executive  
14 Director of Public Policy at AT&T;

15 Fred Cate is Professor of Law and the Director  
16 of the Center for Applied Cybersecurity Research at  
17 Indiana University;

18 Peter Cullen is Trustworthy Computing and Chief  
19 Privacy Strategist at Microsoft;

20 David Hoffman is Director of Security Policy  
21 and Global Privacy Officer at Intel;

22 Joanne McNabb is Chief of the California Office  
23 of Privacy Protection;

24 Hana Pechackova -- I got that right, didn't I  
25 -- is Policy Officer at the European Commission,



1 Directorate-General Justice, Freedom, and Security in the  
2 Data Protection Unit; and

3 Lee Tien is the Senior Staff Attorney with the  
4 Electronic Frontier Foundation.

5 So we basically have four questions we want to  
6 consider in this panel:

7 First, has the market done a good job of  
8 offering privacy and enhancing technological tools to  
9 consumers, and why or why not.

10 Second, how are companies using technology to  
11 protect privacy? Are these efforts adequate?

12 Third, what can and should regulators do to  
13 increase the uptake of privacy-enhancing technologies?

14 And, finally, although we will entertain other  
15 topics if people are interested, how have regulations to  
16 date affected the uptake of the technologies and is  
17 regulation a good way to encourage the development and  
18 use of privacy-enhancing technologies or not, and are  
19 there better ways?

20 So why don't we start with the first. Has  
21 there been adequate uptake of privacy-enhancing  
22 technologies in the market? And I would like Fred and  
23 Lee to maybe discuss this at first, and then other people  
24 can join in.

25 PROFESSOR CATE: Thank you very much, Jessica.

1 And thank you again for the opportunity to be on this  
2 panel.

3 I think the answer, to be honest, is it  
4 depends. And so then it matters on what it depends on.  
5 So it depends on first what technologies we are talking  
6 about. And I think one of the useful discussions we have  
7 had throughout the day is what do we mean by privacy-  
8 enhancing technologies.

9 If we use the broad definition, the way I think  
10 a number of the panels earlier have done, so that we are  
11 including things like spam filters, auditing software,  
12 monitoring software, and so forth, then I think we would  
13 say, yes, we have seen a fair amount of pushing privacy  
14 into products and consumers and, particularly, business  
15 customers willing to pay for those. So look at the  
16 additions to operating systems, to browsers and so forth,  
17 we see a fair amount of privacy-specific or privacy-  
18 responsive technologies.

19 If we define privacy-enhancing technologies as  
20 I think they are more often defined in certainly the  
21 scholarly literature to mean things that consumers buy  
22 that enhance their privacy, then I think the answer would  
23 be no. We have seen a lot of efforts to do that, P3P  
24 being probably the earliest and biggest. And what we  
25 have seen is remarkably low uptake by consumers and a

1 real unwillingness, if you will, to put our money where  
2 our mouths are when it comes time to buy privacy-  
3 enhancing technology as a separate standalone product.

4 MR. TIEN: Yes. I agree with Fred on that and  
5 I want to sort of talk about some of the reasons why  
6 consumers really have not embraced it. And I think  
7 probably the most important is a question of existence.  
8 Does a privacy-enhancing technology even exist for a  
9 given threat.

10 One example that has come up during the day is,  
11 for instance, the question of, say, certain kinds of  
12 supercookies like Flash cookies. For quite a long time  
13 there was simply no available kind of plug-in for most  
14 browsers that could even be used for it.

15 Aside from existence, then consumers actually  
16 have to perceive a threat of some sort and have knowledge  
17 about it even to seek out the use of a privacy-enhancing  
18 technology. On the tech side, many users do not know  
19 anything about these threats. And we actually had an  
20 example in the mobile panel just now about how, well,  
21 what do consumers know about whether or not their GPS can  
22 be pinged or not.

23 On the legal side many users falsely assume,  
24 according to recent research, that their data is legally  
25 protected by the existence of a privacy policy anyway.

1 So, again, you might think, well, if you think the law  
2 protects you, then do you need to get this tool in order  
3 to actually protect your privacy.

4 And then a third reason really is the  
5 inconvenience. If you are not getting your privacy-  
6 enhancing technology as part of your browser and on by  
7 default, you may have to as a consumer go through  
8 installation steps and then actually endure inconvenience  
9 when you are using the Web because, as we discussed in  
10 the first panel, many of the tracking tools that are  
11 threatening privacy are actually part of the way the Web  
12 works. And so when you don't use Javascript or don't use  
13 other kinds of tools, then you are also possibly not  
14 going to be able to use Websites that require them.

15 MS. RICH: Lee, you said that tools just aren't  
16 produced so consumers can acquire them. But it is sort  
17 of a vicious circle. That implies there is no demand for  
18 them. But do you have another explanation for why the  
19 products are not out there available on the market?

20 MR. TIEN: Well, I mean I think there are a  
21 number of reasons. First of all, you need to -- you know  
22 producing software, producing a tool costs resources. So  
23 what is your business model for producing that? We have  
24 seen a lot of tools that are produced, say, by I guess I  
25 would call them altruistic programmers or folks who

1 decide that they want to build this sort of tool in order  
 2 to, say, promote anonymous browsing. You know EFF helped  
 3 support a tool called Tor which is an anonymous browsing  
 4 tool. It actually had been originally subsidized by the  
 5 federal government as part of the Office of Naval  
 6 Research. And because it got some kinds of nonmarket  
 7 support, it actually still exists out there and is fairly  
 8 widely used among privacy-enhancing technologies.

9 But I do not think that it really makes sense  
 10 to think about how the market is going to produce those  
 11 independently of larger equipment manufacturers, whether  
 12 it is the browsers or OSes or whatever. These small  
 13 shops, it is not clear how they are going to get paid.

14 They are not going to be relying on an advertising model

the way a lot of other ent ( s,s 5 -2en a loWecedm .8415 0 TD (14 )Tj 25nk abo/wm .8415 0 -2.2 0 TD-2.

14 0 TD (5) 24B? 0 just T-2. 0Tj ED (W) Dider by Ene Thes m8ll )Tj -2.8415 0 model

1 And now you see, 'We do that on our network because that  
2 is what our customers expect.' But you do not have one  
3 way people are viewing these privacy threats, so what you  
4 have got is a bunch of fragmented demand. And I think  
5 that is another factor.

6 And really I also wanted to underscore this  
7 transparency issue, because we spent a lot of time  
8 talking about transparency as a solution. I think it is  
9 important to recognize kind of the exponential benefit of  
10 that, because through transparency people then understand  
11 if they think it is a threat, they feel threatened, they  
12 start demanding more. And that is this virtuous cycle.

13 MS. RICH: Peter.

14 MR. CULLEN: So this is the right process, my  
15 tent is up; is that right?

16 MS. RICH: Oh, yes, you are following the  
17 rules.

18 MR. CULLEN: Good.

19 MS. RICH: You are following the rules.

20 MR. CULLEN: I liked Fred's parsing of the  
21 definition. And I think it is a really important  
22 question, because if you think about the, I'll call it,  
23 the true disciplinary definition of PETs from, I'll call  
24 it, a European perspective, it does get into this  
25 enhancing mode, which I think Lee touched on a lot. But

1 what I also heard from Lee was a discussion about or  
2 questions about the effectiveness of this.

3 I'm not sure that the metric of market adoption  
4 is necessarily the right one and I think there was a  
5 comment made earlier that the fact that these tools are  
6 available actually promote trust. And that is a  
7 different thing than saying that they are only effective  
8 if people have taken them up.

9 And I would argue that even the opt-out method  
10 is, by Fred's definition, some form of privacy enhancing.  
11 The fact that very few people take advantage of the opt-  
12 out is not a metric to say that the market has failed, it  
13 is a question to say that I think that consumers value  
14 the availability of these sorts of privacy enhancements  
15 that do not necessarily feel that they have to take  
16 advantage of it.

17 MS. RICH: Hana.

18 MS. PECHACKOVA: I would like to share our  
19 experience from the European Commission point of view.  
20 We have launched a study on economic benefits of privacy-  
21 enhancing technologies. We are somewhere in the middle.  
22 We have the first interim -- the second-interim report,  
23 and there were quite interesting lines why that did not  
24 really take up yet and what are the major problems.

25 It is not about threats only, it is more about

1 information sharing, about information failures. Because  
2 companies, they tend to withhold the data, not to really  
3 inform the public about breaches of laws, about the data  
4 leakages unless they really have to, unless it is a legal  
5 obligation. So that is why we are looking at the  
6 possibilities to introduce into our law the obligatory  
7 notification of a data breach. Because if you really see  
8 clearly that there were cases, and there are cases, it is  
9 happening every day, that there are cases, then there are  
10 some leakage of data, of course you would have a very,  
11 very good business case for deploying privacy-enhancing  
12 technologies, for really taking it seriously and looking  
13 at that. It is not only about threats, but you really  
14 have to see that there are problems in practice in  
15 everyday life. So this for me is one of the reasons and  
16 it has also been confirmed by our researchers.

17 MS. RICH: So it is transparency not just on  
18 the consumer side but on the business side?

19 MS. PECHACKOVA: Exactly, yes.

20 MS. RICH: Lee?

21 MR. TIEN: Yes. I just wanted to add a couple  
22 of meta points. I mean one is that I don't think  
23 privacy-enhancing technologies in sort of a market-  
24 adoption area is really going to be a particularly  
25 powerful answer to consumers' privacy problems. It is not





1 this information, but really to make a larger enforcement  
2 feedback loop actually work.

3 MS. RICH: Thank you.

4 Fred.

5 PROFESSOR CATE: I would certainly echo that  
6 point and, frankly, would also go back to an earlier  
7 point that Lee made, and then Hana's comment made me  
8 think maybe was worth coming back to accentuate, and that  
9 is one of the reasons we may not see market take-up of  
10 sort of traditional privacy-enhancing technologies is  
11 because there really are not technological solutions to a  
12 lot of the privacy issues. That it is a mismatch, if you  
13 will.

14 And Hana's example of security breaches made me  
15 think of this entirely. I cannot imagine why security  
16 breaches would motivate more consumer take-up of privacy-  
17 enhancing technologies given that security breaches  
18 involve companies that typically lawfully have the  
19 information, need to have it, or have it for a reason.  
20 There is nothing I can do. I can buy all the privacy-  
21 enhancing technology I want, put P3P on, set all my  
22 browser settings. Nothing is going to help me in that  
23 situation.

24 So the traditional view of privacy-enhancing  
25 technologies would say they are just useless in terms of

1 the types of situations that I think today has helped  
2 kind of hone that people really worry about. We have a  
3 good example here. I mean we have had a notice of  
4 security breaches of course in California for four years  
5 now -- well, how long has it actually been in effect, has  
6 it been seven?

7 MS. McNABB: Seven.

8 PROFESSOR CATE: Seven. So we have the expert  
9 here.

10 Yet we do not see California running out to buy  
11 privacy-enhancing technologies. There has been no  
12 tremendous P3P upsurge here. Not because -- that  
13 wouldn't be a rational response to that. And so I doubt  
14 if we are going to see privacy-enhancing technologies  
15 picked out as an irrational response to these types of  
16 threats.

17 MS. RICH: Well, what you are talking about,  
18 though, is a good reminder that, and Hana's remarks too,  
19 that privacy-enhancing technologies are also very  
20 important on the business side, if you think of them more  
21 broadly. And I think -- David has his tent up and he is  
22 also well situated to answer TD gk9Pashow are businesses  
23 doing using technology to protect data and how are they  
24 ensuring that it gk9used at the earliest opportunity so  
25 that it gk9not superimposed on existing systems so that



1 do.

2 MS. RICH: Well, so besides encryption what are  
3 you doing to protect data?

4 MR. HOFFMAN: Well, that is an interesting  
5 question. For us a large amount of the data that we  
6 have, right, is the data we are storing on our backend  
7 servers in our enterprise systems. So this then 'What  
8 are we doing to protect data' gets into a large  
9 discussion about what are we doing for cybersecurity. It  
10 is not just about protecting personal data but it is  
11 about protecting our intellectual property and the data  
12 that we use to run our business.

13 I think there is a tremendous amount of  
14 investment going on across the board for companies there  
15 and a tremendous amount of investment of trying to  
16 intersect development life cycles -- I know we are going  
17 to talk about this a little bit later -- but to do that  
18 earlier and earlier so you are not bolting on things  
19 later. And I know that has gone down to the vendors,  
20 that the vendors who make this enterprise software, for  
21 example, are baking that in.

22 It happens at the hardware level for the things  
23 that we produce and I think software vendors would say,  
24 could talk about the tremendous investments that they are  
25 putting in and protecting that data.

1 MS. RICH: Well, I do want to talk about baking  
2 it in at the earliest opportunity. Peter, are you  
3 prepared to talk about that?

4 MR. CULLEN: Yes, I can.

5 I just want to make sure, Lee, do you want to  
6 continue on this point?

7 MR. TIEN: I wanted to throw in one quick  
8 point. And, again, it is like the point about notice of  
9 security breaches and what Fred was saying, at EFF we are  
10 always recommending to folks if you don't have the data  
11 you can't be forced to give it to the government and you  
12 can't leak it or anything like that. And having the  
13 opposite of data retention, data deletion as a policy, as  
14 a practice is something that, you know, really doesn't  
15 require any fancy new tools. It is just something that  
16 people could do, would be very cheap, and would mitigate  
17 a lot of privacy problems. And we need to think of  
18 incentives, more incentives for doing that.

19 MR. CULLEN: So I think there is ample evidence  
20 over the past decade, to even 15 years, to suggest that,  
21 well, there is a market in the customer's face for what I  
22 will call true privacy-enhancing technologies. It is a  
23 relatively small one. Whereas what has happened over the  
24 past four to five years, particularly in the business  
25 case, is a much greater demand for privacy or data

- 1 protection type technologies or informational governance
- 2 type technologies and solutions. So certainly as a
- 3 provider of those sorts of things, we are seeing a great  
demand for that.eing a great

1 company does business. Our previous model that I am  
2 talking about even sort of six or seven years ago of  
3 perhaps relying on lawyers to review products as they  
4 were going out the door really just did not prove to be  
5 very tenable.

6 So this way of designing into the process  
7 allows for, I'll call it, the stated objectives to be  
8 met.

9 I think the other kind of maybe splitting back  
10 into the privacy enhancing for the community was simply  
11 to make those standards publicly available and to start  
12 to build them into other lifecycle type transparency  
13 communication things, making them available for other  
14 software developers, the way that we have thought about  
15 it. So this really is a complete but very prescriptive  
16 cycle, at least from Microsoft's perspective.

17 MS. RICH: What are the incentives for  
18 companies to have more privacy-enhancing products? I  
19 think in many ways we are also talking about defaults, --

20 MR. CULLEN: So --

21 MS. RICH: -- which was the subject of a lot of  
22 discussion earlier.

23 MR. CULLEN: Yes. So I think there is --

24 MS. RICH: And what are the disincentives too?

25 MR. CULLEN: Yes.



1 MS. RICH: I want to get at both.

2 MR. CULLEN: So Microsoft is perhaps different  
3 from other companies in the sense that, like all  
4 companies, there is an expectation that we have robust  
5 protection around and appropriate use of information, but  
6 I think that where the difference is that consumers and  
7 businesses expect us to provide them with technology that  
8 helps them protect their information. So I think there  
9 is a different motivation from Microsoft's standpoint.

10 I think the fact that we do not have -- you  
11 think of kind of an operating system, there really is not  
12 a direct relationship with a consumer. There is an  
13 arm's-length relationship. It means that the trust  
14 perception, the trust relationship is much more difficult  
15 to obtain. So from our standpoint the onus is to be that  
16 much more trustworthy in there.

17 I think the other advantage that kind of we  
18 have found from our experience of building it into the  
19 development lifecycle is it actually generates privacy-  
20 enhancing capabilities. And I will use an example of a  
21 review on the phishing filter.

22 And the model was, wow, in order to provide  
23 dynamic protection from phishing, we need to collect IP  
24 addresses from users simply because the market of  
25 phishing is just so dynamic that is the only way to do





1 that you know.

2 And so what was interesting about what they did  
3 was they, through this guidance document, sent a message  
4 saying: Get better at this or there is going to be some  
5 substantial disincentives for not having better tools  
6 here.

7 What I think is particularly interesting about  
8 that is the effect that that has had throughout industry.  
9 So the banks then went to the folks who provide the  
10 authentication services for them and said, 'We're hearing  
11 this; we need better tools for doing it.' Those  
12 companies then ended up coming to us for hardware, other  
13 software companies saying, 'We need better privacy-  
14 enhancing technologies.' And now what we are finding as  
15 a result of that, that we have got projects pretty far  
16 along coming out of our labs at this point to provide  
17 some very good hardware-based, and I know there is also  
18 software-based, further methods of authentication.

19 So I think that is an excellent example where  
20 you have got the trust on the one side working as an  
21 incentive, but then selected disincentives that come from  
22 regulatory agencies or quasi-regulatory agencies to  
23 create even the specter of the disincentive, which pushes  
24 things along.

25 MS. RICH: Okay. Well, Joanne, you have got

1 your tent up. Do you want to -- are you going to address  
2 the incentives and disincentives? Sort of.

3 MS. McNABB: I think so. Yes. Yes.

4 Just building on what David said, his  
5 mentioning the authentication regulation ultimately, but  
6 first just raising the issue. In a way that same  
7 approach is what the breach-notification laws, it is the  
8 way they have operated. It did not say you have to use  
9 these things to protect information. It said -- it  
10 created, it revealed a price, the price of having bad  
11 security, bad privacy practices, and it shifted the  
12 burden of paying that price from the victims, whose  
13 information, as Fred said, they could not have done  
14 anything to protect, onto the party that could do  
15 something.

16 I think one of the reasons that the market, one  
17 of the factors in why the market has not kicked up more  
18 PETs, is that that sort of -- the actual costs have been  
19 hidden, the costs to consumers have been hidden in many  
20 cases.

21 MS. RICH: Hana.

22 MS. PECHACKOVA: I would like to briefly talk  
23 about incentives, but about the role of the regulators,  
24 because it is up to us, the regulators, to show that they  
25 are not --

1           MS. RICH: We are definitely going to get to  
2           the role of the regulators, but I just wanted to sort of  
3           finish up with more the businesses' own incentives, even  
4           outside of regulation. Everyone is dying to talk about  
5           regulation, which is very interesting. He's bursting out  
6           of the crowd, even the companies. But...

7           MR. CULLEN: Let me take an I-agree-with-  
8           Joanne-and-I-disagree-with-David scenario. I can  
9           disagree with David, but I do not disagree --

1 ability to read mag stripe read cards,' and they said,  
2 'Well, no, because consumers do not have the keyboards  
3 and the cost of rebuilding our infrastructure is just  
4 really prohibitive for us to do that. And, besides,  
5 right now in an online transaction, the cost of the fraud  
6 is actually born by the bank, not by us.'

7 So we go to the bank and say, 'Well, why don't  
8 we do this,' and they say, 'Oh, well, actually, no. If  
9 we do that, it actually makes it a card present and that  
10 actually might move the liability really, really to us,  
11 so there is no real motivation for us.'

12 When we go to the regulator and say, 'Boy, you  
13 have got this industry and guidance about two-factor  
14 authentication, why don't you use this as an example. It  
15 would have such a dramatic impact on this,' they say,  
16 'No, no, no, we can't interfere in the market.'

17 MR. HOFFMAN: So I actually don't think you are  
18 disagreeing with me. I think we agree, which is there is  
19 a role for the regulators to play to encourage the things  
20 that are fundamentally broken and that that plays a great  
21 role within the market.

22 MR. CULLEN: I am relieved because I do not  
23 like to disagree with you. That is good.

24 MS. RICH: Okay. Well, we got to go to the  
25 regulation because that is what everyone wants to talk

1 about. I know these guys have things to add on that, so  
2 why don't we talk about what is the role of the  
3 regulators in encouraging the uptake of these  
4 technologies both on the business side and to offer to  
5 consumers. So, Hana, I know that you have spent a lot of  
6 time thinking about this. You have done a lot of work  
7 with the European Commission to promote privacy-enhancing  
8 technology and privacy by design, so can you talk a bit  
9 about that?

10 MS. PECHACKOVA: Yes. Sure. The European  
11 Commission did a lot of work in this field. We did a lot  
12 of research. We invested lots of millions of euros into  
13 the research. We did it together with our colleagues  
14 from Direct Regional Information Society and Media. The  
15 research in this field started, if I'm not mistaken, back  
16 in 2002. It was under the Sixth Framework Research  
17 Programme. They were interesting studies and interesting  
18 research, like PRIME or FELIS (phonetic). Now we are  
19 running the Seventh Framework Programme, and again a lot  
20 of millions of euros are invested. But it is not only  
21 the research of the European Commission, it is usual  
22 there are public contenders and we are working together  
23 with industry on how to get it right. But we are also  
24 launching some other studies to look at the policies,  
25 what we can do to bring the privacy-enhancing



1 technologies into policy and how to regulate, whether we  
2 should introduce it into new laws or not.

3 It took us some time to create in Europe to  
4 build our democratic values, it took several generations,  
5 but now with the new technologies of course you have to  
6 foster those values and bring them to the digital era, to  
7 the digital age, but how to do that.

8 So we are currently looking at the future of  
9 privacy, the future of protection of personal data in the  
10 EU. In the last year, in July 2009, we have launched and  
11 brought online public consultation. And the EU received  
12 very good feedback. We received more than 160 replies  
13 from individuals but also from associations and from  
14 companies. So one of the lines were that we have new  
15 technologies that are challenging our values, but we  
16 could also use some of those technologies to help us,  
17 because you cannot address everything only in the law.  
18 So the technology could be kind of a complementary mean  
19 to help us to get it right.

20 So we have to be innovative and we are looking  
21 at what to do because we do not want to step back of  
22 course from our values, but we have to make our legal  
23 regime more workable and more adjustable to the current  
24 situation. So ideally we would introduce new principles  
25 which would be, for example, the principle of privacy by

1 design, which is one step ahead of the privacy-enhancing  
2 technology. So we would absolutely support that. That  
3 then would be privacy-enhancing technologies but in a  
4 broad sense of course, because when you have privacy-  
5 enhancing technology you have kind of two phases of that.

6 The first one is before you implement you think  
7 really twice. And then when you already implement the  
8 technology and then after that you embed some enhancing  
9 tools into that. So we also wanted to supported this by  
10 the study on the economic benefit, because it's our role,  
11 the role of regulators to give incentives, that we just  
12 talked about. And we want to show of course -- you  
13 mentioned trust. Trust is of course the backbone of the  
14 information society. And the data are circulating by  
15 business every second around the globe, so this is very  
16 important for us. It's not only about trust, we have to  
17 show that there are economic benefits. And if there are  
18 economic benefits, we would make not only companies but  
19 also public sector to use it because we are looking not  
20 only at the private individuals or at the private  
21 company, but they are also looking at the government  
22 level.

23 It is also very important that the government,  
24 the public sector implements the privacy-enhancing  
25 technologies because the trust in there would really give

1 uptake of all the economic applications, it would help to  
2 save money again for the public sector. And if you show  
3 the incentives it will be of course ideal situation.

4 And then on other principle would be the  
5 principle of accountability, but we can take long hours  
6 about accountability.

7 MS. RICH: Thanks.

8 Joanne, California's been in the forefront of  
9 privacy and security regulation. Has there been a focus  
10 on encouraging privacy-enhancing technologies either in  
4 your state or others that you know of?0

1 consumers, it was usually at legislator meetings, for  
2 example, who were coming to hear about identity theft.  
3 So these were privacy fundamentalists or privacy-  
4 activated people. And we would ask them questions and  
5 have a raffle and give away a shredder at the end. And,  
6 oh, they were thrilled.

7 Well, after about two years everybody already  
8 had a shredder. So I mean the consumer uptake definitely  
9 occurred. And there is a whole industry that is not  
10 called the shredding industry, it is the information-  
11 destruction industry that goes from shredding papers to  
12 crunching up and recycling computers and beyond, and does  
13 a lot of education on the laws that require you to do  
14 that.

15 MS. RICH: And you supported those laws.

16 MS. McNABB: Yes, indeed.

17 MS. RICH: So, Ellen, to what extent has your  
18 company and others like you been influenced to adopt  
19 privacy-enhancing technologies because of regulation, or  
20 not?

21 MS. BLACKLER: I was going to talk about the  
22 kind of conundrum we have got here is that it is hard, it  
22 is a really complicated ecosystem, it moves veryl, rh3kly,

22

1 kind of to throw up your hands. But I think that we have  
2 seen some success. You guys put a pretty big spotlight  
3 on behavioral targeting over the recent past and put out  
4 the self-regulatory guidelines.

5 And I think not to overstate any of that, but  
6 the industry kind of hopped to. And I think we have seen  
7 over the last couple weeks with the National Privacy Day  
8 and the workshops these announcements about things that  
9 maybe are not going to solve the problem but took  
10 cooperation across a range of folks in the ecosystem that  
11 would not have had happened absent the spotlight you  
12 shined on it. You know, the icons that will now be used  
13 in advertising that will start to get at the technology.  
14 I think the introduction of the profile managers by some  
15 of the big ad network companies. You know all of that is  
16 because of the spotlight that the regulators shined on  
17 it, which then made, I think, consumers wonder what was  
18 happening. And the combination does result in a focus on  
19 privacy.

20 Now we at AT&T are not in the ad network  
21 business really so much, so we do not do too much of  
22 that. But where we did enter the business we made sure  
23 that we had a profile manager and we had separate notice  
24 and we had these kind of what we call table stakes to get  
25 into the business because you guys said these are table

1        stakes, get into the business.

2                So I think that is an important way to balance,  
3        to weave through the need to not be prescriptive but also  
4        have something. The privacy by design I think is another  
5        emerging issue that is going to be hard for a company in  
6        the near future to not have an answer to what is your  
7        internal process for making sure privacy is considered.

- 1 on -- to encourage privacy-enhancing technologies, are
- 2 there things that people can do right, government can do  
right or the things that government can do wrong?

1 saying, 'I can't code reasonable.' And then they're  
2 jumping -- there would generally be two or three lawyer  
3 jokes thrown in as they swore under their breath.

4 But then the reply that I got good at giving  
5 after a while, after I thought about it, was to say, 'All  
6 right, do you really want the lawyers designing the  
7 product? Is that what you're really' -- and the answer  
8 was really no, but the engineers were actually pretty  
9 good at solving problems if you give them the problem  
10 that you want them to solve and you provide them with  
11 some freedom to figure out how to do that. And I think  
12 that's been the direction where we have seen regulation  
13 that has moved in the right way. It is regulation that  
14 has said: Here is a problem and this is unacceptable.



1 MR. HOFFMAN: -- know other people have  
2 comments, I think underneath that then you have  
3 relationships between the regulators and industry and  
4 academics and NGOs about how do you provide guidance  
5 underneath that so that David Hoffman's not talking to  
6 the engineers and trying to make up all on his own what  
7 he thinks reasonable is. But that is not necessarily  
8 part of the regulation. We talk about that as a sort of  
9 triangle of trust with those entities coming together to  
10 figure out some of those problems.

11 MS. RICH: And consumer.

12 MR. HOFFMAN: Indeed.

13 MS. RICH: Lee, do you want to address this  
14 issue?

15 MR. TIEN: Yes. I just wanted to jump in and  
16 sort of -- while we have been talking about government's  
17 role here as sort of a regulator that is attempting to  
18 protect privacy, we just cannot forget that there are a  
19 lot of roles the government ends up playing that are  
20 actually pretty harmful to privacy. The U.S. government  
21 has just historically discouraged encryption technology  
22 deployment in the United States for a long time.

23 We have seen that there are technologies that  
24 are being deployed by local governments, state  
25 governments, as well as the federal government, such as

1 RFID, that are almost designed to expose information  
2 about where people are. Right now in California we are  
3 looking at the expansion of the FasTrak RFID-based toll  
4 transponder system which is not only insecure but relies  
5 essentially on a system that is going to be tracking  
6 people's location at least as they are crossing toll  
7 bridges and any other points where sensors are.

8           And what is ironic about this is that we know  
9 that in the EU people are looking at very interesting  
10 private tolling methods. We know that commercially  
11 available there are crypto-based systems where you can do  
12 this kind of automatic tolling with complete anonymity.  
13 But trying to get, say, a state agency like CalTrans to  
14 even sort of notice this or to get this sort of truly, I  
15 think, designed-in privacy into these systems is not an  
16 incredibly easy thing.

17           The third example I will use here is, again,  
18 data retention, right. I mean we have all recognized  
19 that deleting data protects privacy. And yet again the  
20 federal government is actually -- very often law  
21 enforcement will tell carriers in the telecommunications  
22 world, 'Hand over data. Keep data.' It is not clear  
23 whether or not it is actually even useful for law  
24 enforcement for data to be kept for six months or two  
25 years, or whatever.

1                    We hear that after 30 days probably is really  
2                    most in the utility of it, and yet if the government is

1 have taken -- because the lawyers have been told to worry  
2 about Social Security numbers, and so the lawyers have  
3 translated that through into business processes when the  
4 real message if we were going to send a regulatory  
5 message, should be: Worry about the management of  
6 sensitive data, whether that's personal or other types of  
7 sensitive data so that you can all sorts of disincentives  
8 that are necessarily bad. Maybe "disincentive" is the  
9 wrong word. But they're just tangential, they are taking  
10 us away from the core focus.

11 I think a second point is we need, and I  
12 understand this is the whole point of these workshops, so  
13 I am just stating the obvious and I want credit for  
14 stating the obvious, we need a little more clarity on  
15 what are the objectives.

16 In other words, nobody wants the government  
17 promoting a specific technology and I'm sure the  
18 government doesn't want to do that either. It will be  
19 out of date by the time -- but what we need are very  
20 clear objectives. And so security, and I think this  
21 point has been made clearly, but again it is worth  
22 echoing: That is clearly an objective I think we all  
23 agree on. And, therefore, some notion of accountability,  
24 of liability, if you have data and you do not secure it  
25 so that it is used in ways that cause some form of harm,



1 Nobody wanted to pay for those.

2 So I don't think we necessarily want the  
3 government saying, 'That was a mistake. The market  
4 should have worked. We are now going to make you or  
5 incentivize you to go buy this technology.'

6 On the other hand, there is a lot the  
7 government can do to make technology work better. And I  
8 have thought about this all day while we have been  
9 talking about anonymization and deidentification, and so  
10 forth. In most areas of law outside of this sort of  
11 privacy area, deidentification is paralleled with very  
12 strong laws.

13 So, for example, FDA research. If I do  
14 research I have an identifier for every research subject.  
15 And if I inappropriately link those -- it's easy. I can  
16 just go get it and compare them. It's not that it's  
17 technologically hard, it's that it's a felony to do so,  
18 and that law is enforced rigorously. So that's a law  
19 that backs up a technological process, anonymization or  
20 deidentification. And I think that is quite a useful way  
21 to think of law.

22 The last thing I would say and then I will just  
23 go home and you will be done with me, is to think about  
24 the roles other than regulation. And I think Lee was  
25 really making this point. The one, I'm of course the

1 academic on this panel, I always think of as fund  
2 research. I understand the FTC is not likely to go out  
3 and establish a multibillion dollar fund for research on  
4 privacy-enhancing technologies, but we do have a problem  
5 in that a lot of the research that the government does  
6 fund, largely through the NSF in privacy, is not focused  
7 on anything applicable.

8           You could take it all and add it together and  
9 say this will never make one bit of difference in terms  
10 of enhancing privacy. It is fascinating research. And I  
11 live off that money. I am not encouraging us to get rid  
12 of it. But nobody -- I mean those projects are not  
13 reviewed on the basis of will these make a difference,  
14 they are reviewed on the basis of will they advance the  
15 state of knowledge.

16           But another role the government can play, and  
17 again I think Lee was getting at this, is by using  
18 privacy-enhancing technologies, so that if the government  
19 said we are going to go in the market for certain types  
20 of privacy-enhancing technologies, that would be probably  
21 the greatest incentive the government could create,  
22 rather than saying, 'We're going to regulate for it' or  
23 'We're going to fund the development of it.'

24           Thank you.

25           MS. RICH: Well, I do want to comment, though,

1 that just -- I mean we have talked earlier about why  
2 there hasn't been an uptake of privacy-enhancing  
3 technologies on the consumer side. There definitely  
4 appears to be on the business side in that you are using  
5 technology to protect data.

6 But you could get -- I am sure somebody could  
7 give you an argument that its failure in the marketplace  
8 does not mean there is no demand for it, that this could  
9 be an area of market failure, that you had to mandate --  
10 the law had to mandate seatbelts -- see, now maybe I will  
11 get you all exercised. But does anybody want to give him  
12 that argument?

13 Hana.

14 MS. PECHACKOVA: It's a kind of circle because  
15 of course the consumers, they will not start using the  
16 privacy-enhancing technologies or buying them or putting

22m on their computers unless they had to use the technology. The 24 and so 2.81 nawhadTj - m2.2678 TD ( f2 MS. PEC  
9m on their computers unless they had to use the technology. The 24 and so 2.81 nawhadTj - m2.2678 TD ( f2 MS. PEC



1 we have to find incentives, I would say, more for  
2 companies, why to deploy and use them in their business  
3 processes. I think this is very important. But it's  
4 kind of really a circle, so we have to start somewhere.

5 MS. RICH: Joanne.

6 MS. McNABB: Well, I think as Lee said a while  
7 ago, one of the reasons he believes the market has failed  
8 to produce a wonderful array of PETs for consumers is  
9 that they are -- what has been produced and why there has  
10 not been a big uptake, what has been produced is not  
11 conveniently available. Well, isn't built into the  
12 browsers, et cetera.

13 Well, wouldn't it be one of the factors here in  
14 the marketplace that the business models of much online  
15 business is to increase the collection of personal  
16 information, that there is a disincentive to facilitate  
17 people being able to do more things without providing  
18 personal information, which is a kind of privacy-  
19 enhancing technology that is different from protect the  
20 information once you've already got it from people. It  
21 is antithetical to the business model.

22 MS. RICH: Peter.

23 MR. CULLEN: I thought you weren't going to  
24 pick on me, because my tent was up and you are worried  
25 about me misbehaving.

1 MS. RICH: I am alternating between differing  
2 viewpoints.

3 MR. CULLEN: Oh, okay. So I think your market  
4 question is a really interesting one, and let me pick on  
5 two of your examples, just to illustrate this.

6 You used or raised the specter of seatbelts.  
7 So it has been a law in certainly most states if not --

8 MS. LEFKOVITZ: The initial point was consumers  
9 would not pay extra for seatbelts, right, so the  
10 government -- and so car manufacturers said, 'Well, we're  
11 not going to put them in because consumers won't pay  
12 extra,' now government had to regulate, so --

13 MR. CULLEN: But it is an example of --

14 MS. LEFKOVITZ: -- it's all bundled the price.

15 MR. CULLEN: It's an example of where you have  
16 a law that says you have to wear it. There's been, for  
17 20 years or so, there's been an incredible amount of  
18 education.

19 The downside of not wearing a seatbelt is  
20 pretty real: You die. Yet still only today 80 percent  
21 of Americans wear seatbelts.

22 Antivirus. There are huge business models. I  
23 mean there's huge companies that make business out of  
24 this. It comes as part of your PC as a free service.  
25 Still today 30 percent of consumers are only running

1 active antivirus. So I think we have got it recognized  
2 this is a multifaceted problem.

3 But I want to get back to the technology-policy  
4 reasonableness question because I think this is where  
5 part of the problem exists. To Fred's point, technology  
6 policy will inherently fail, for lots of reasons. One is  
7 that it's complicated. Two, that the technology  
8 solutions are often outdated, and they're really fixing a  
9 very small problem. I think this gets back to even -- as  
10 I was reflecting upon the conversation throughout the  
11 day, we are doing this deja vu all-over-again model where  
12 we find an issue, whether it be social networking today,  
13 whether it be Flash cookies tomorrow, whether it be RFID  
14 yesterday, and we continue to have this debate about what  
15 technology solutions might be available or what  
16 regulation is needed.

17 We are not having this conversation under the  
18 banner of a framework, and let me use data-breach  
19 notification to illustrate this. Many people would argue  
20 this is a successful piece of legislation, but it's akin  
21 to thinking about what do we do with the horse once it's  
22 left the barn. Nobody has actually thought about what  
23 are the standards that help secure the barn. And when I  
24 say standards that help secure the barn, it strikes me  
25 that one of problems we have is that we need to vacillate

1 between this prescriptive versus descriptive manner. And  
2 I think this is to Fred's point.

3 The BT guidance has actually been a pretty good  
4 example of a descriptive motivator that helped the  
5 industry come together and think of actual solutions to  
6 this. When you get prescriptive, it becomes problematic.  
7 But I think to say stop at the reasonableness standard,  
8 that's just not good enough because that leaves just too  
9 much open. So be more descriptive, I think, is the  
10 potential solution to this, but within a framework.

11 MS. RICH: So if reasonableness is too high  
12 and --

13 MR. CULLEN: No, reasonableness is too vague.

14 MS. RICH: Too vague. And then a very specific  
15 standard around a particular technology is no good, is  
16 something -- what if you mandated privacy risks  
17 assessments, is that coming in at the right level? What  
18 if you had a standard like data minimization, could  
19 technology -- would that spur technological solutions to  
20 make sure you are not keeping or collecting too much data  
21 and keeping it? I mean at what level are we talking  
22 about?

23 MR. CULLEN: Let's -- let's actually --

24 MS. RICH: Maybe Lee. Maybe -- yeah.

25 MR. TIEN: I guess, I mean, I love the concept

1 of privacy-enhancing technologies, but what I care about  
2 is enhancing privacy. And I don't care whether it's with  
3 technology or regulation or with some other kind of  
4 regime.

5 And I think one of the reasons why we dance  
6 around the standard is because it's a very hard thing to  
7 actually sort of work out, what would be optimal. And  
8 that is the sort of thing that privacy advocates will  
9 fight -- will all be fighting about it. And it would  
10 take time to work out.

11 But I think that what's -- I guess I don't have  
12 a whole lot of stomach for the idea of sort of having our  
13 privacy be on in that kind of a process when I think that  
14 what we need to think about is liability rules and  
15 enforcement.

16 You know we spent a lot of money -- or a lot of  
17 time thinking about what the rights, say, of privacy and  
18 security rules were for health information in HIPPA. And  
19 they might be very good, I don't know. But what I do  
20 know is that for quite a few years and HHS received tens  
21 of thousands of complaints of HIPPA privacy violations,  
22 and I think acted on two.

23 It does not really matter what standards or  
24 rules we come up with if we do not actually have a  
25 genuine commitment of resources and political

1 institutional will to enforce those standards, and I  
2 think that's going to -- that's going to have to include  
3 in our system actual civil liability through private  
4 rights of action. You know Paul brought that up and I  
5 think that that's a part of your ingredient.

6 I mean in my view one of the most effective  
7 privacy laws of all time, although that may not be so  
8 true anymore, had been the Wire Tap Act. The Wire Tap  
9 Act was a law that made very clear that the act of  
10 intercepting electronic or wired communications was  
11 unlawful. You did not have to prove harm, you just had  
12 to show this bad behavior occurred. It has -- you know  
13 Congress authorized -- civil suits, persons aggrieved for  
14 that. And normally, and it is also backed by the Justice  
15 Department, which actually criminally prosecutes some of  
16 these things. And that's -- I think our own litigation  
17 aside, the history of the Wire Tap Act as a privacy  
18 protector I think is actually not that bad because it  
19 sets a clear rule and it has clear compliance  
20 possibilities.

21 The only thing that I would add is I think that  
22 in this era where we do need to make sure that the kinds  
23 of private rights of action we create definitely include  
24 mass tort type actions, class-action type vehicles,  
25 because otherwise you are not going to be able to really

1 -- I would much rather rely on the efficiency of some  
2 sort of a private class litigation than of the political  
3 whims of whether or not a state attorney's general, et  
4 cetera, et cetera, get involved.

5 MS. RICH: Ellen, what do you think  
6 policymakers should do to encourage privacy-enhancing  
7 technologies? In the broad sense.

8 MS. BLACKLER: I wanted to go back to what  
9 someone over here said about objectives, that if we had a  
10 clear objective you can kind of work through with the  
11 people who build product, how to mean it, and kind of  
12 balance this need for creativity.

13 I think maybe some of what's happening is the  
14 objectives have shifted and they haven't been well  
15 articulated. So we -- the FTC is talking about notice  
16 doesn't seem right anymore. And so what is the new  
17 objective? I think we have been circling around this  
18 idea of transparency. People have talked about that  
19 today as different than disclosure. Telling me what  
20 you're going to do in a privacy policy is not  
21 particularly transparent, but having a customer see  
22 what's happening when it's happening. And if you said to  
23 the engineers, 'Find a way for consumers to see that,'  
24 maybe you would get some answers that we can't come up

1 with today.

2 And I guess I would add to that list of  
3 objectives this usability notion because I think that's  
4 where some of the technologies have not -- it goes to the  
5 adoption issued to me. Some of these are not hard  
6 technological answers. What's hard is making them usable  
7 to customers. And if we put some focus on that, we might  
8 also see some innovation.

9 MS. RICH: Let me stay with you then in that  
10 you -- your industry took a hit on packet inspection,  
11 being the gateway -- being a gateway to consumers and so  
12 much information. Is there a special role that you and  
13 others like your company can play in providing these  
14 protections through technology, because of the gateway  
15 rule that you play.

16 MS. BLACKLER: Well, we try not to use that  
17 gateway word. But since you have said it, I think we  
18 have looked closely at the market opportunity here. And  
19 one of the things that has come clear to us actually is  
20 that there's -- for some reasons I mentioned earlier.  
21 There is actually not really so much that a network  
22 provider can do that fixes the solution, because there  
23 are so many ways the consumers can get at these products.

24 And I think someone mentioned earlier -- or I  
25 guess it was Alissa who said earlier you have an apps



1 store, for instance, and maybe the applications on the  
2 apps store have been vetted and live up to some standard.  
3 The consumer can go to the Internet and have this exact  
4 same kind of capabilities happen with a whole different  
5 set of protections.

6 So it's really not as simple as finding kind of  
7 this silver bullet in the network, particularly when you  
8 keep in mind the consumers don't all want one thing. So  
9 where we've kind of started to coalesce is around is  
10 really this individual-control notion. And the  
11 opportunity for us as a gateway provider, really exists  
12 for other gateway providers. And it is really your trust  
13 relationship with the customer because they're paying  
14 you, they have high expectations of you, you're setting  
15 up service for them, and so that's an opportunity to  
16 educate them and maybe get their privacy preferences that  
17 you can then, on their behalf, help them work through  
18 their Internet experience. But that is probably the same  
19 for any a device owner, for a platform owner; anyone with  
20 that kind of direct customer relationship, I think, has  
21 the opportunity.

22 And it kind of goes back to what David said  
23 when we talked earlier about competing on privacy. I  
24 think it is actually a lot more complex for the customer.  
25 And you're competing on trust, not really privacy. And I

- 1 think the customers have a sense that privacy is part of
- 2 their trust relationship, but it's really only one part.



1 these particular areas and then you go back and you  
2 evaluate again to see if your systems are working, et  
3 cetera. So it is more specific than reasonableness.

4 At least in the data-security area, has that  
5 model actually spurred greater use of technology to  
6 protect data?

7 MR. HOFFMAN: Well, I would want to change your  
8 question. I think what I want to say is has it created  
9 more use of technology or has it increased better use of  
10 technology through the use of better business process.  
11 From what we see, we go out and interview all of our  
12 customers' customers, the chief information officers of  
13 the major company is out there, and the answer is clearly  
14 yes.

15 If you went back ten years and you asked what  
16 the processes were around information security and you  
17 looked at what they are now in these companies, it's  
18 lightyears ahead. And I think the FTC played a big role  
19 there.

20 MR. CULLEN: So just --

21 MS. RICH: That's a good way to be ending this  
22 panel.

23 (Laughter.)

24 MS. RICH: Well, Fred has his card up a long  
25 time. Can I go to him?

1 MR. CULLEN: Can I just close with -- just with  
2 one thing?

3 MS. RICH: Oh, but you've conspired to go?  
4 Okay.

5 MR. CULLEN: Yes. I mean David just kind of  
6 articulated what I'll call this tripod. In the business  
7 sense it's people process and technology. I know you  
8 have asked the question a lot of times about technology,  
9 but I think it is really important to say that technology  
10 is just one part of a solution.

11 If you think about it from the consumer angle,  
12 it's a combination of technology, education, and some  
13 form of regulation or government policy.

14 MS. RICH: Fred.

15 PROFESSOR CATE: I am just a little concerned  
16 that we not end by having totally abandoned the side of  
17 consumer privacy-enhancing technologies because I think  
18 we need to be clear about the failing so that we have a  
19 better understanding of if there is a role what that role  
20 might be.

21 I don't think anybody can prove there has not  
22 been a market failure here. But if you look at the  
23 available evidence what we know is that not merely are  
24 consumers not buying this stuff, they're not using it  
25 when it's given to them, so it doesn't look like a market

1 failure.

2 In other words, when my browser says, 'Don't go  
3 to this Website, we think it's dangerous, and it turns  
4 the bar red at the top,' and we know because the  
5 researchers are in this room who do that research that  
6 people click right through those, we're not talking about  
7 the government mandating the technology, the government  
8 would have to mandate that I follow the technology or it  
9 would have to say Microsoft now has to ship Explorer that  
10 shuts down when I don't do what it says to do. It just  
11 seems like we really have a serious problem here on the  
12 consumer side of privacy-enhancing technologies.

13 So if they are going to play a role, and it's  
14 particularly not all together to clear to me that they  
15 are except as bundled, it's going to be a really tough  
16 road to hoe to get them in place, since we know that even  
17 when they're there we can't get people to use them. And  
18 I am not talking about complicated places like my  
19 firewall where I don't know what it means when it asks  
20 will I accept this communication on port 45, you know I  
21 know what it means when it says, 'We think this is a fake  
22 Website.'

23 The other sort of piece of this I guess I would  
24 just reflect on, I rarely, in fact I virtually never  
25 disagree with Lee, but I would not at least as a starting

1 place look for mass tort litigation as a good place to  
2 start here trying to create incentives. Not because I  
3 don't think it can play any role at all, but because I  
4 think there are a lot of better places.

5 And you know it was frankly right here at Boalt  
6 Hall a year ago that we had the breach conference. And  
7 at that time I think it was 165 class action litigations  
8 on breach notices, not one of which had there been any  
9 damages found in. I have no idea whether there was harm  
10 or not, I'm not arguing that one way or the other. What  
11 we know is that there have been hundreds of million of  
12 dollars of attorneys' fees spent, if there had been harm,  
13 no individual had been compensated. And as much as I  
14 love attorneys, and I really do and I think they're  
15 fabulous, and I'm sorry that people have criticized them  
16 on this and other panels, but --

17 (Laughter.)

18 PROFESSOR CATE: -- I think it is a better  
19 place for the Commission and frankly other regulators to  
20 think about setting forth clear standards, leading  
21 processes that lead to clearer standards, identifying  
22 objectives rather than starting with let's let courts try  
23 to figure out on their own in kind of the mass tort  
24 litigation setting.

25 MS. RICH: Well, I really don't want to end on

1 a court point, Lee, do you --

2 MR. TIEN: Well, I wanted to point out that I  
3 was not -- I did not mean to imply that that would be  
4 like the only thing. What I meant to say is that, and  
5 maybe even did say, was that this was simply one  
6 particular -- one thing that should not be automatically  
7 excluded from the pallet of tools. And because what we  
8 have had over the last several years has been quite a few  
9 instances of seeing that we just don't get enforcement  
10 from a whole variety of places where you might expect  
11 enforcement or you might expect to try to get liability.

12 If we really do agree that this is a problem,  
13 then we should try to practice sort of a multiple  
14 redundancy strategy in terms of how we are going to get  
15 to the optimum level of precaution in society rather than  
16 attempting to sort of hit the bullseye right now, which  
17 can take five, ten years, and then you are not sure you  
18 are going to get there anyway. I think there is  
19 something to be said for a little bit of organized chaos  
20 in this area.

21 MS. RICH: Well, I actually want to end on -- I  
22 have to end, but I want to end on the people, processes,  
23 and technology point because that's a refrain that we use  
24 at the Commission all the time too. And it's a good way  
25 to end this second roundtable because this roundtable is



1 about technology, but it's really part of the larger  
2 whole of people, process, and technology in privacy.

3 So thanks to the panel. And we're going to  
4 have Chris Olsen come up for some brief closing remarks.  
5 Thank you very much.

6 (Applause.)

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

1 CLOSING REMARKS

2 ASSISTANT DIRECTOR OLSEN: Thank you to the  
3 last panel. I am going to make you all sit here for at  
4 least a few more minutes. I will be brief.

5 Before I provide a few remarks I must thank  
6 everyone who worked so hard to put this event together.  
7 Of course it would not take place without the assistance  
8 of Chris Hoofnagle, Robert Barr, David Grady, and Louise  
9 Lee at Berkeley, as well as the Berkeley law student  
Cy43.9oaEnn (3 )zLiz ErplaaviVivian Kim, Colin HectoaviYan -2.24048415D (1 )Tj0 2.24048415D678 TD (

1           We also heard about emerging developments like  
2           digital signage. We explored in more detail a topic  
3           raised at our first roundtable, whether personal data may  
4           truly be anonymized, and we examined the development of  
5           privacy-enhancing technologies and their role in  
6           protecting consumer privacy. This led to a lengthy  
7           discussion of genies and bottles. Who would have  
8           thought.

9           One point that came out of this panel is that  
10          technology alone may not be sufficient to protect  
11          consumer privacy interests and that they have to be --  
12          they may need to be supplemented by policy solutions.

13          Our social-networking panel started with the  
14          discussion of the many benefits of social-networking  
15          services. It featured a healthy debate about consumer  
16          exceptions and the extent to which extensive sharing of  
17          personal information is well understood by consumers.  
18          Some said clearly yes, some said clearly no.

19          We spent a great deal of time examining third-  
20          party application issues. We heard the comment "data is  
21          the lifeblood of applications." We looked at the issue  
22          of who bears responsibility for the privacy and security  
23          practices of third-party apps. Is it the platform, is it  
24          government regulators.

25          Finally, we examined the portability issue and

1 whether consumers can easily transport their online lives  
2 to another site. If portability is difficult, does that  
3 give platforms a freer hand to change the rules of their  
4 service without losing customers?

5 Our cloud computing panelists focused on  
6 enterprise uses of cloud and examined the privacy issues  
7 raised by the falling costs of data storage and the ease  
8 with which it may be maintained over time. Again we  
9 heard a quote similar to one we heard on the social-  
10 networking panel: "More data is always better than less,  
11 and we'll figure out what to do with it."

12 We also debated the wisdom of greater  
13 transparency for business practices in the cloud and  
14 noted the jurisdictional complexities that we have to  
15 keep in mind as we move forward.

16 Mobile computing focused us on two significant  
17 issues: The extent to which location-based services were  
18 proliferating really in an explosive way, but perhaps in  
19 an environment without consistently-applied rules or  
20 standards. And the degree to which transparency of  
21 information-sharing practices is happening successfully  
22 on mobile devices.

23 There was some agreement that some consistent  
24 principle should apply here but perhaps not consensus on  
25 what those principles should be.

1           And, finally, our last panel explored the  
2 intersection between technology and policy and Fred's  
3 love affair and hate affair with lawyers. Building on  
4 the discussion in the first panel, our last group of  
5 experts discussed ways in which our policy framework may  
6 create incentives to protect privacy interests and to  
7 build privacy protections into new products and services  
8 at the outset.

9           We heard from our international colleague about  
10 progress that the EU has made on this front and I am sure  
11 there are lessons for us there.

12           That brings us to an end for the day. Our  
13 examination of rapidly-developing technologies like  
14 social networking and cloud and mobile computing may call  
15 to mind at least for some what historian Lewis Mumford  
16 said about technology years ago, "Western society has  
17 accepted as unquestionable a technological imperative,  
18 not merely the duty to foster invention and constantly to  
19 create technological novelties but equally the duty to  
20 surrender to these novelties unconditionally, just  
21 because they are offered without respect to their human  
22 consequences."

23           Our expert panelists deserve our gratitude for  
24 helping us examine these technological issues and their  
25 human consequences. We look forward to equally robust

1 and engaging discussions at our third and final  
2 roundtable in Washington on March 17th. We hope to see  
3 you all there and we thank you again for coming.

4 (Applause.)

5 (The Roundtable was adjourned at 6:06 p.m.)

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

## 1 CERTIFICATION OF REPORTER

2 PROJECT NUMBER: P095416

3 CASE TITLE: PRIVACY ROUNDTABLES

4 HEARING DATE: January 28, 2010

5  
6 I HEREBY CERTIFY that the transcript contained  
7 herein is a full and accurate transcript of the digital  
8 audio recording transcribed by me on the above cause  
9 before the FEDERAL TRADE COMMISSION to the best of my  
10 knowledge and belief.

11  
12 DATED: February 11, 201013  
14 \_\_\_\_\_  
15 SUSAN PALMER16 CERT 00124  
17

## 18 CERTIFICATION OF PROOFREADER

19 I HEREBY CERTIFY that I proofread the transcript for  
20 accuracy in spelling, hyphenation, punctuation, and  
21 format.

22  
23 \_\_\_\_\_  
24 NANCY PALMER

25 CERT 00121