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

INDEX

PROCEEDINGS

- - - - - -

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

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

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

(Applause.)

PROFESSOR MULLIGAN: Thank you. All right.

Good morning. On behalf of the Berkeley Center for Law and Technology and the Berkeley campus more broadly, it is an absolute pleasure to welcome the privacy community to Boalt Hall. It's an honor, in particular, to host this second of three Privacy Roundtables on behalf of the FTC because of its strong focus on technology as both part of the drivers of change, as well as a potential place to search for solutions.

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

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

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

And I was fortunate enough to be at the very first workshop about kind of what were the emerging consumer issues going to be in this new marketplace. And Chris and I were talking with our students and they were, like, what were people doing on the Internet in 1995.

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

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

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

The information that we are posting, the associations that we are revealing, and all of the information that can be gleaned, the knowledge that can be created that this is no longer just data, this is fodder for a growing knowledge economy, and how do we maintain some semblance of a private life, some semblance of separation as we have these social networks?

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

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

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

And, finally, I want to give you a little bit of logistical information. Bathrooms straight back on the left. Question cards in your folders. If you are participating online, PrivacyRoundtable -- all one word -- @FTC.gov.

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

She's been very prescient and forward-looking, looking to see where the market's going, not just what the privacy issues are today, but how they are going to be changing and presenting as we move forward, and I think incredibly perceptive about the connections between privacy and antitrust and privacy in a market economy. And for all those reasons I think that we are really privileged to have her kicking off our meeting today.

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

(Applause.)

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

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

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

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

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

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

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

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

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

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

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

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

One of the biggest growth areas is the mobile space, which is generating incredible amounts of data. Given the exponential increase in penetration of mobile devices and services, mobile privacy is crying out for greater attention. Think about it. Worldwide every day more people use mobile devices than use the Internet.

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

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

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

When the app is downloaded and installed there is no mention of privacy. Mr. Widner asked the software developer whether users had contacted them to ask about security, and the developer responded that he had received almost no inquiries about the security of the app or where their details were going.

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

Suppose the average user has 15 third-party applications, each written by a unique developer with a different privacy policy or, likely, no policy at all. How likely is it that users truly understand how their privacy will be affected by what they have downloaded?

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

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

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

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

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

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

Consumers may not even understand when or how they are using cloud services, especially with respect to hybrid applications that have both cloud and desktop features. As data passes through the cloud it is entrusted to multiple parties. The obligations and accountability of these caretakers must be clearly spelled out to ensure that sensitive data remains safe through the chain of custody and control.

Among other safeguards, cloud service providers must employ secure transmission protocols and establish strong security defaults. Consumers also should be more mindful of potential lock-in concerns that may arise when competitors utilize incompatible or proprietary standards and formats.

This problem may be magnified or amplified when data is fed into so-called free services. Users must understand what rights they have over their data. And where providers do promise that affordability, consumers must be allowed to move their data without hassle.

In closing, I would like to briefly explore one particular issue that I hope will inform any later discussion of privacy-enhancing technologies, and that is the concept of anonymization. I call to your attention an insightful and potentially groundbreaking paper by Professor Paul Ohm at the University of Colorado.

Professor Ohm articulates what he views as the failure of anonymization, because he has found that simple computer science techniques enable supposedly hidden data to be reidentified or deanonymized. Professor Ohm's work mirrors the work of researchers at the University of Texas at Austin, who have detailed the use of seemingly anonymous information to uncover the identity of Twitter users on the Netflix rental service.

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

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

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

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

(Applause.)

DIRECTOR OLSEN: Thank you, Commissioner Harbour.

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

(Applause.)

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

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

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

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

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

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

First, that consumers have little understanding of commercial information collecting practices. They don't really understand what data is collected about them, how that data is used and shared, and whether and how they can exercise control over their data.

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

Indeed, one panelist summed up the extent of consumer confusion. He noted a survey showing that when consumers see the phrase "privacy policy" on a company's Website they think that that means that the company does not share their information with anyone else. We must find ways to improve consumer understanding.

A second and related point is that, although traditional, lengthy privacy notices drafted by lawyers are not effective communication tools. There remains an important role for privacy disclosures. Industry is coming up with interesting innovations in this area.

Some panelists discussed the possibility of development of a universal icon which would alert consumers that behavioral advertising is taking place. Other panelists discussed new models of consumer disclosure like those offered by Google and Yahoo!, where consumers can see which categories of advertising they receive and opt out of receiving information and advertising in specific categories.

At the same time, panelists expressed concern about the extent to which consumers are aware of these options; very few take advantage, as well as the extent to which consumers could easily navigate multiple, different company systems to offer transparency and control.

Third, the last thing that we already knew, that consumers do care about privacy, was driven home in many different ways. Several panelists discussed surveys showing that consumers are uncomfortable with the practice of behavioral advertising.

Beyond surveys, we know that consumers take affirmative steps to protect privacy, particularly when surfing online. In fact, one panelist mentioned that Ad Block Plus, a pop-up blocker, was the most downloaded add-on for Firefox.

And just last week I noticed that the number one emailed article from the New York Times Website was an article about how consumers can change their privacy settings on Facebook, the number one emailed article. That fact speaks volumes about consumers' interest in their own privacy.

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

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

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

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

But it raises some challenges, and we are going to talk about those today. Indeed, our opening panel will delve into this very issue: How can technology enhance consumer privacy and how it might challenge or circumvent consumer privacy, the double-edged sword.

Here, we will explore what we see as a troubling consumer privacy arms race. For every tool developed to give consumers control over collection or tracking, it seems that a counter measure is quickly developed to neutralize or defeat consumer choice. We need to explore that phenomena.

Then our panels will examine three questions in specific context: Social networking, cloud computing, and the mobile environment.

First, social networking, the online equivalent to the water cooler. Social networking has, and there is just no doubt about it, has revolutionized the way we interact with people.

Who needs a Hallmark card when I can poke someone online, or why should I send out an annual holiday card to my friends and family when I can update them on my life online in real time?

On the other hand, these sites are a boon to consumers, enabling us to reconnect with high school friends, look up old flames if you have any, or cement relationships with potential business partners.

On the other hand, of course, it means that others can scrutinize the minutia of our lives, future employers, current bosses or, even worse for my kids, their parents might try to friend them.

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

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

At the same time, storing data on remote computers raises serious privacy and security concerns. For example, the ability of cloud computing services to collect -- excuse me -- to collect and centrally store increasing amounts of consumer data, combined with the ease with which such centrally-stored data may be shared with others, creates a risk that larger amounts of data may be used in ways not originally intended or understood by consumers. Our panelists are sure to shine some sunlight on this practice of cloud computing.

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

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

Our last panel will highlight ways in which companies are building privacy into their products and services at the outset, in the way policymakers can encourage such practices. Ideally, privacy protections will be baked in at the beginning, rather than be half-baked afterthoughts.

Before we begin the first panel let me make one final comment. I don't want anyone to think that the only work the FTC is doing on privacy is reflected in these roundtables. These roundtables are a pillar of our policy formulation going forward, but they do not represent the sum total of our work in privacy.

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

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

(Applause.)

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

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

PANEL 1: TECHNOLOGY AND PRIVACY

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

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

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

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

In the escalation of technologies to be used in ways to improve our lives we have begun to see that there are ways in which they may also detract from our privacy.

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

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

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

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

We are going to look at advances in technology that challenge our assumption about how anonymity works and what it means in a technology-driven world where it may be possible to amalgamate individual bits of data and recombine them in ways that lead to identification of people who previously thought they could not be known.

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

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

So with that I am extremely pleased to tell you that we will be talking today with eight expert panelists. The panel will be moderated today by myself, Catie Harrington-McBride, from the Federal Trade Commission; my colleague, Loretta Garrison. And with us, we are joined in alphabetical order because, after all, it's the only fair way to do things, by these eight excellent panelists. We have with us:

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

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

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

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

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

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

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

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

Scott Taylor, who is the Chief Privacy Officer at the Hewlard -- Hewlett-Packard company. Sorry about that, Scott. And:

Anne Toth, to Scott's left, Vice President of Policy and head of privacy at Yahoo!

So we have an esteemed panel, and we hope to engage in a very vibrant discussion.

A couple of announcements just by way of procedure to let you know how this will work. It will be a moderated discussion. Lori and I will be asking questions of the panelists, sometimes calling on them individually, sometimes throwing something out for everyone to fight for.

We will certainly encourage all of our panelists to participate, regardless of whom we may have called on first. And, panelists, just to remind you, if you have something that you would like to say, would like to jump in the mix, if you could just raise your table tent so that we know that you are interested, we will certainly try to call on you.

We are going to have to keep a close watch on the time, although we have the most generous allotment of the entire day, I'm proud to say. No doubt, Lori and I have muscled the others on today's panel to give us this extra 15 minutes. We have so much to cover that we may need to cut things short. So just let us know if you have an interest in speaking, and we will certainly try to get to you.

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

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

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

So we would be delighted to hear from you. We will try to incorporate your questions to the extent that time allows. And with that I think I'd like to kick it off with some questions. Our panelists know, because we have been doing a lot of prep calls, that we have a strong interest in talking about technologies that are sometimes new, but sometimes repurposed.

And by "repurposed," what we mean is a technology that was actually developed for one reason, of course, and then is being reused for another. And a good example of that seems to be the use of Flash cookies or local, stored objects for a purpose that they were not originally intended. And so we wanted to talk a little bit about that.

There have been a lot of recent studies on this, a lot of press coverage, and we wanted to ask, how did Flash cookies come to be used instead of HTTP cookies, and what are the privacy implications of their use. So for that, Peter, would you like to start us off?

MR. ECKERSLEY: Sure. Flash cookies function a lot like the ordinary cookies that your browser will accept and then send back to a Website you visited previously. But the difference is that rather than being built into the browser itself, they are built into the Flash plug-in that was produced by Adobe.

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

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

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

MS. HARRINGTON-McBRIDE: Thank you.

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

PROFESSOR HOOFNAGLE: Yes. As Peter mentioned, the Flash cookies are not controlled by the browser settings. And this was an advantage, according to some advertising companies. In fact, there is a press release from one advertising company that simply says consumers don't know about this avenue, and we can track people even if they delete their cookies.

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

(Laughter.)

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

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

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

MS. HARRINGTON-McBRIDE: All right. Sid?

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

MS. HARRINGTON-McBRIDE: Pam.

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

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

But does this change the privacy problem that's been identified by the studies and that some of you have mentioned here this morning?

MR. ECKERSLEY: I think it only partially addresses the problem. The fact remains that if you go into your browser and say, "Delete all cookies," the Flash cookies are still there. And the fact remains that if you go into your browser and say, "Limit cookies to the current session, if I quit my browser I want the cookies to go away," Flash still doesn't respect those, those requests. So I mean, they have taken one step towards fixing the situation, but they have got more to do.

MS. HARRINGTON-McBRIDE: And to be clear, this is not -- I mean, I think that Chris Hoofnagle raised this point -- this is not something that Adobe is doing. This is something that advertisers are taking advantage of in the Adobe technology. Sid, did you have something?

MR. STAMM: Yes. I'd like to make a comment on this new privacy mode. The reason that Flash didn't address a private browsing mode in the past was because the Web browser and the Adobe Flash plug-in are essentially two separate programs, and they don't really communicate a whole lot.

And so in order to get it to listen to the browser when the user wants to enter a private browsing mode we had to create some sort of signal the browser could send to Adobe Flash to let it know, hey, the user wants to be in private mode.

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

MS. HARRINGTON-McBRIDE: Anne?

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

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

so I think if you look at the role of self-regulation here, companies are basically raising their hand and saying, we will not do this. And it's just another point of differentiation.

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

MS. HARRINGTON-McBRIDE: Okay.

PROFESSOR HOOFNAGLE: A minor point.

MS. HARRINGTON-McBRIDE: Um-hum.

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

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

(Laughter.)

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

PROFESSOR GOLDMAN: I think the discussion about Flash cookies is really just a microcosm of that introductory remark about a technological arms races. And so, as usual, we have to ask the question: What will technology do to cure the problem itself, or the market will do to cure the problem itself, and whether we need the FTC to fill in the gaps.

And so Chris' point may be valid that perhaps we would say that the market will never fix the problem with respect to the third-party relationship. But I look at the Flash cookies as an opportunity for technologists and market players, like Yahoo!, to say: Here's how we are going to respect consumers' expressions of interest.

And, you know, when we have the next version of this panel x number of years from now, we'll be talking about some other things, but we are going to have the same deja vu of, there has been a gap created between what technology can do and what consumers want, and what should we do. Should we fix it? Should we wait for someone to fix it? I think Flash cookies are just a small microcosm of that broader problem.

MS. HARRINGTON-McBRIDE: That's an excellent point that Eric raises. We also want to talk about other means of using existing technologies or perhaps developing newer technologies to find new ways to collect data. And, again, some of these are nonopaque. Some of these are perhaps in circumvention of consumers' wishes.

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

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

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

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

But what we have got is the -- and Microsoft

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

Now, some of them, some of them do better jobs at respecting user preferences. I know that Mozilla tends to block the dumb-storage cookies, if you block cookies. So I don't want to say that all of these as a category are as bad as the Flash cookies are.

But there is this constellation of potential tracking mechanisms, a whole cloud of potential tracking mechanisms that people need to worry about. And, you know, as a consumer advocate I don't want to tell people, hey, go and do these ten things and then spin around backwards in order to not be tracked.

MS. HARRINGTON-McBRIDE: Pam.

MS. TOTH: You know, when I think about cookies -- and I haven't had breakfast yet. So I'm actually -- a supercookie sounds really good to me right now.

(Laughter.)

MS. TOTH: But I want us to all be cognizant and think about not throwing the baby out with the bath water. So there are lots of benefits that technology imparts on us. And, you know, if you block all cookies you will actually not be able to take advantage of some of the value that cookies provide to you and that exists, you know, in the Internet space, but offline, as well.

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

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

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

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

MS. HARRINGTON-McBRIDE: Scott.

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

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

And I think what's being highlighted just in this first discussion is the fact that technology itself isn't necessarily bad, but we have got to ensure, as Anne was highlighting with Yahoo!, that organizations are held accountable to understand the risks that these technologies pose, as well as the benefits, and that they are held accountable to the obligations and the promises that they make, whether those are driven by regulation or their own self-assertions.

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

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

So I think that that concept of accountability and administrative controls really is going to be some place we need to focus on if we are ever going to try to solve the problem of the good and the bad, the double-edge sword that Commissioner Harbour talked about.

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

Pam, you have some new research on that. Could you tell us a little bit about what you are seeing?

MS. DIXON: Sure. We put out a report yesterday that details, I think for the first time, the profound privacy issues in digital signage networks. These are basically networks where video screens are bidirectional as opposed to unidirectional.

You have a good example in Whole Foods in Chicago. People who are walking around looking at tomato videos are actually having their images captured by the video screens, analyzed by facial recognition technology, then having their gender analyzed and sent back to the mother ship for direct marketing purposes.

Now, I don't think that the people looking at the screens at Whole Foods in Chicago exactly know that this is going on. I looked at the privacy policies in Whole Foods. No disclosure of this. Not that someone would be cruising around looking at produce thinking about a Website privacy policy in the first place. So this raises a lot of issues.

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

So what does this mean for consumers? The big problem here is that your face, your body, your gender, your ethnicity, your personal characteristics become new data fodder. And when you look at what these companies are saying about how they are managing the data in their code of best practices and also in their privacy policy, what they have come to is that faces and people's bodies are no longer PII, or personally-identifiable information.

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

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

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

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

Apparently, you don't need to shop online for that to be the case, according to this new information. This is an emerging field. Does anyone else on the panel --

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

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

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

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

MS. HARRINGTON-McBRIDE: Anne.

MS. TOTH: I think that as we think about these things, restrictions on use rather than perhaps even collection might be more useful. So if I'm at Whole Foods and they notice that I'm looking at tomatoes and they notice that the same individual, not knowing necessarily who it is, is looking at lettuce and they put tomatoes and lettuce together, well, I might be okay with that. That doesn't feel very invasive.

But if they are doing that in order to market to me in a very personal way where they know who I am or they have matched it to my actual identity, then I have some other issues with it. But those things have happened for a very long time now. And, you know, I work in this industry. I think about these issues all the time.

It wasn't -- it was sort of driven home to me for the very first time after I had a baby, and I showed up at home with this brand new baby and waiting for me at home was a giant can of infant formula mailed to my home, to my personal address, knowing that I had just given birth to a baby.

And I sat there and I thought, wow, you know, they didn't waste a second, you know. So direct marketing practices like this that know who you are, that associate it with some potentially sensitive information, I think some people might think giving birth to a baby is kind of personal, but it's a public-record event, right?

That's the sort of thing I think that starts to get people a little bit concerned in that form of use.

MS. HARRINGTON-McBRIDE: Chris, your thoughts?

PROFESSOR HOOFNAGLE: Just to follow up on that point. One of the things that's interesting about privacy-enhancing technologies is that they are generally -- or at least in my experience -- there have been generally restrictions on collection. The whole idea behind pets is just to stop information collection.

And so I would pose a question: How could we use technology to ensure that uses, use controls, are followed, because I think that the problem that many consumers face is that once that data gets out they really have no control over use. And there is no kind of transparency in some of these organizations. There is no data provenance.

So how do you ensure that once this data goes out as a consumer or as a regulator can technology be used to ensure there use restrictions are in place?

MS. TOTH: Something potentially audacious. Yes. We at Yahoo! have developed tools to let users see what we think you are interested in, right? So we have our Ad Interest Manager that we launched a month ago, and it is a privacy-enhancing technology. We are trying to use technology to empower consumers to say: This is how you know what we know and this is how you control what we can use about you.

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

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

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

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

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

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

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

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

But to air a little bit more about the specific issue of tracking, I mean, Anne raises the point that, you know, this is not maybe secret data anyway. Shopper loyalty cards and other mechanisms perhaps allow for some transparency already.

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

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

DR. NARAYANAN: I was going to make a point about the distinction between collection and use. Maybe I can wait for another --

MS. HARRINGTON-McBRIDE: Okay. Pam.

MS. DIXON: Yes. I think there is a hierarchy that you can really look at in terms of this technology. Some tracking technologies pose less risk. Some pose a lot more risk. But right now, already in practice, we have systems that are tying your captured video data with facial recognition, with gender analytics, to loyalty card purchases. It's already happening right now.

So that information becomes identifiable. And I think something that we need to think about, is that we are really moving into a world where images are going to become the new identifiability. You know, instead of your name being the big idea online, it's going to be your image.

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

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

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

MR. ECKERSLEY: Excellent. Thank you.

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

Even if we could actually implement them all, there are other kinds of regulation or help that we probably need in order to get consumers some privacy back. But having said that, the fair information practice of access is a really interesting one and one that I think, if we could do some more work in developing it and implementing it in a sensible way, might be a powerful light to shine into the kind of dark void of data collection.

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

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

And the other hard thing that it would need to do is that it would need to be secure. See, because if you just build this thing and you don't do it securely, then hackers and people who want to collect data about people will soon be sneaking in there and getting your data out of it.

But if we can solve those two problems then I think this would be an exciting direction to explore in terms of giving consumers more control.

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

MS. GARRISON: Well, thank you.

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

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

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

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

And in that sense technology has, I think, made things a lot better to where it's been very helpful to, you know, lots of peoples around the world.

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

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

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

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

PROFESSOR HOOFNAGLE: Yes. And this relates back to the previous discussion. There are very subtle ways in which people can be uniquely identified, as Arvind has pointed out in his academic research. But I'd call everyone's attention to a recent case called Pineda v. Williams Sonoma, here, a California state case.

In this case, Jessica Pineda went to a Williams Sonoma store and paid with a credit card. And at the register the cashier asked her, "What is your ZIP Code?"

And what was going on behind the scenes is that Williams Sonoma was taking the ZIP code and combining it with her name capture from the credit card swipe, and that actually gives you unique identification, or at least unique enough for marketing's sake.

So even, you know, even when you are at that register and someone asks you your ZIP Code, what might be going through the consumer's mind is, do I need to provide this for security, for authentication. The underlying issue there, the underlying motivation might actually be identification in such a way that it hides it from the consumer.

MS. GARRISON: Well, now, we have this merging, also, of -- we not only have the richness of all this data that's being collected offline through video and other kinds of new technologies online, but we have the merging of the data. Traditionally, the privacy law has focused on this distinction between what is personally-identifiable information and that's what's to be protected and secured, and then nonpersonal identifiable information where you don't have as great a concern because it doesn't link to an individual.

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

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

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

Some data never will have any real impact.

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

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

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

MR. TAYLOR: Yes. I think that it's a good example, and it's a good question. The example of being able to identify somebody and to create some impact is really what I'm talking about. So data can be combined, and that data suddenly becomes personally identifiable. The data by itself in different sources may not be. And we have talked a lot about IP addresses.

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

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

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

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

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

Each bit of data may not be interesting in itself, but it has some sort of significance towards the person's identity, the person who owns the data. And with enough of these little bits of data you can end up with something that's personally identifiable.

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

Arvind.

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

One is in breach notification laws, which a number of states have passed recently in response to incidents of theft of sensitive data such as Social Security numbers and credit card numbers.

Now, breach disclosure laws lay out these categories of what the laws call PII. And those are the categories of data which, if breached, then consumers need to be notified.

There are also privacy laws, which are about a completely different issue. It's not about financial information. It's about all information in general. In these laws they also use the term "PII," but in a very different way. Sometimes they do lay out categories, but even when they do they follow it up by saying that any information that can potentially be used to reidentify should be considered PII.

And what the research has shown, as Sid just mentioned, is that any bit of information at all can have that role in conjunction with other pieces of information. And so if we are going to talk about PII at all in the context of privacy it must be admitted that all information is PII. And, basically, that is why I feel that this concept does not have both.

MS. HARRINGTON-McBRIDE: Peter.

MR. ECKERSLEY: Conveniently, to add to what Sid and Arvind have been saying, which sounds like a confusing morass, like how could we cope with a world where every single fact is potentially identifying. It turns out there is a fairly elegant mathematical theory for doing that.

And I don't want to talk about mathematics too much on this panel, but those bits, if they are independent of each other, can be added up. And the mathematics is if you hit 33 independent bits of information about a person's identity that's enough to make them globally unique on this planet with seven billion people.

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

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

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

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

MS. GARRISON: Anne, I want to throw a question to you that's related to this. Should we care whether data can effectively be identified, or should we change consumer expectations and accept that there is ubiquitous collection of all information about us, no matter the source, whether it's publicly available or privately held?

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

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

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

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

So I think that from a pragmatic standpoint as businesses we have to make decisions based on resources and what's practical to do. So that's an important consideration. I just want to make sure that we think about that. I think there are lots of -- when I read a lot of these articles I think they are fascinating, but I also know that, you know, we have strong policies in place to do the best we can to prevent some of those things from happening. And we should be held accountable to those policies.

Now, in terms of ubiquitousness of data that's being collected, I think, you know, as Pam has pointed out, we are all exuding data all the time, right. And that is a challenge for us, not just online, but in the offline world.

We are walking around, and I'm exuding data at this very moment. It is a challenge for us. And I'm not sure that there is going to be one easy solution to say: This is how we educate consumers about those things. I do believe that consumers need to understand more about what's happening and need to understand how they can control these things.

When we talk to consumers about online privacy, there is a great deal of fear and confusion about it. And I think it's largely been because it's the Internet. It's technology. I don't know who's there. I don't know how it works. It's a black box. But I think consumers actually aren't entirely aware of just how much else in their world is equally as complex.

If I walk into a room I think, well, I know I can see everybody in this room. So I have some sense that I'm controlling my presence in this room, but I can't control what everybody does with what they are hearing from me and when they walk out of this room what they think about me, certainly. So there are some natural limits to that.

MS. HARRINGTON-McBRIDE: I just have a brief announcement. There is apparently a two-door, red, Toyota Camry parked behind the law school, but you didn't leave the keys. So if that's one of you, could you please go to the rear and somebody should be able to talk to you about that.

Pam.

MS. DIXON: I think something that's intriguing about PII is that the definition of what constitutes PII is definitely in motion most of the time. And certainly one innovative way of addressing that would be to go the HIPAA route, which views information, all information, as protected health information or essentially PII.

The healthcare sector has managed to survive that and deal with it. I think two very practical things that can be looked at, one, is that I think we need to spend more time thinking about how do we remove PII and how frequently do we remove it.

I think some of the problems that we have been talking about today start to go away if companies start to shed the data. And if, for example, companies were to collect personally-identifiable information, and defining that very broadly, but were to shed that data within 24 hours I think some of the privacy risks may be diminished.

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

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

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

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

Eric.

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

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

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

And I don't mean to speak for Yahoo!, but perhaps we might even go so far as to say that the privacy manager systems that you guys offer would fit into the bucket of a privacy-enhancing technology. It's designed to try to make the consumers' experience better, to get the information they want and keep the information they don't want.

I don't know if you would consider it that way but, certainly, we could be very expansive in how we think about that. So if we think about it expansively when we look at the "history," we actually have to look at the full set of different ways that people would try to manage their information flows. And I think that actually shows some successes and some failures.

MS. HARRINGTON-McBRIDE: Okay. Anne.

MS. TOTH: Thank you for that segue. The thing about it when we look at advertising online it's one small area of data collection and use online, but the Ad Interest Manager that we introduced is one piece of that.

One of the things that we were looking at is, you know, how do you enhance notices. How do you make them? How do you put them outside of privacy policies? The announcement of the industrywide icon, you know, is an example of movement towards trying to simplify and educate consumers in a consistent way across the industry that when you receive an ad online you can go and look at this icon, click on this icon and find out ultimately -- and this is the direction we are moving in is actually -- by transmitting some meta data about the ad with the ad.

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

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

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

That is, I think, our challenge. And we are, I hope, stepping up to the plate and providing one model for how that can be done.

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

Does anyone take issue?

Peter?

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

So one example of that is the Web. And if you look at the Web and the privacy threats that we find in the Web, they start with IP addresses, which were necessary to make TCP connections, to fetch data from a Web server. They include the third-party content that can see what you are doing, which came from the desire to make the Web a hypertech system, so that content from different places could be combined.

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

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

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

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

MS. HARRINGTON-McBRIDE: All right.

Sid.

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

So our philosophy is that privacy matters and people like to be able to opt out of these things. And so in Firefox, for example, we have been making it central that the user can control all the data that goes out about them through various features like Private Browsing Mode.

We have redesigned the way that people clear history and cookies so that it's more user friendly and actually understand what's going on. And we basically think that anything we can do to give people better control over data that's transmitted off their computer onto a Website is something that they are going to want. And the difficulty arises in making it so that it's usable. And we have a lot of efforts in that area.

MS. HARRINGTON-McBRIDE: Scott.

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

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

So I think that privacy by design, as Commissioner Harbour was talking about earlier, comes in many forms, not just for the end user, but for organizations themselves to help make sure that they do what they say.

MS. HARRINGTON-McBRIDE: Pam.

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

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

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

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

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

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

If you look at the history of privacy-enhancing technologies it's been really successful for that five-percent minority, but not so much for what economists call this pragmatic majority. And good examples of both of those would be, I'm again going to bring up Tor, that's only a small percentage of the people who are in a sufficiently privacy critical situation to go to the extent of installing and using Tor. And it's done a great job for them.

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

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

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

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

Katie, you started this vein of questions by invoking the history of this issue. And I think one of the things that's worth looking at is the 1996 staff report, which discusses self, which discusses PETs in detail. And I doubt any of us could even name the PETs that were on the table back then, but they included predecessors P3P.

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

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

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

Are these PETs usable and can people with a lot of incentives, ad networks, et cetera, to undo those technologies, are they able to circumvent PETs? If we started out with some benchmarks here we could come back to the next roundtable five years from now and we could say: Have we made any progress or not?

MS. HARRINGTON-McBRIDE: Sid.

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

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

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

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

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

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

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

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

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

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

MS. HARRINGTON-McBRIDE: Okay. Eric.

PROFESSOR GOLDMAN: I think the question you are asking is who owns the responsibility to provide the shield that consumers might want. And let's just toss out two other possibilities.

One is the operating system that sits on everyone's computer, and two is the merging of antispyware, antispam, and antivirus software.

Right now, typically those are siloed, but ultimately we all know that doesn't make any sense. And so there is going to be another group of entities that will be out there providing this type of shield functionality to consumers. I think the question for each of those, whoever we pick here, is what regulatory overlay will apply to.

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

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

MS. TOTH: I just wanted to point out consumer attitudes vary a lot and consumers are fascinating creatures. You have a small percentage who care incredibly deeply about personal privacy and then you have the people with the Webcams in their bathrooms, you know.

So you have this wide array of different attitudes about privacy. Most consumers are in the middle, right? Most consumers are. And I think one of the interesting benefits of privacy-enhancing technologies is that they are there for the small percentage of users who will actively engage with all the settings and use them.

But they actually do, I think, provide a great deal of comfort for the majority of users who may never visit them, just to know that they are there and that they can access information and they can control how some of this information is used. I feel like we are sitting -- we are sitting in this great law school, and you can't help but think about what a very wise man once said and that, you know, sunlight is a great disinfectant, right?

So just knowing that it's there, knowing that I can see it, knowing that no one's hiding this from me is a very powerful thing for consumers to know. They don't all have to use it to feel a lot more comfortable just because it exists.

MS. HARRINGTON-McBRIDE: Scott.

MR. TAYLOR: I just wanted to go back and say that I don't think there is a killer app at all. And I really appreciate Eric's comments about the fact that -- he's mentioned it a few times throughout the discussion this morning -- that, you know, the proliferation of technology is not helpful if you can't bring it together and solve the problem in one place, whether that be a browser, an operating system, whatever it may be.

That theme is coming out clear to make it easy and in one place to be able to provide meaningful control or transparency.

But Chris brought up the point earlier that, you know, we should think about P3P. And I absolutely believe that there's all kinds of technologies that could enhance privacy that are out there right now that could be leveraged and deployed.

But if we don't have regulation and industry codes of conduct that are providing a framework and an incentive for organizations to implement these controls in meaningful ways, the technology by itself is going to be meaningless, or it's going to be effective, but in silos and not across the board.

And in the end that's just going to create more confusion or a false sense of security. We really have to ensure that there are -- you know, the technology sits at the bottom as an enabler for other things, whatever those incentives may be, grand reputation from a company, the ability to share information freely and robustly to drive innovation, or regulation itself.

There is a place for all of these things to come together to help provide not only the framework, the requirements or the incentives, but the technology needs so that we can actually design it to do something meaningful.

MS. HARRINGTON-McBRIDE: All right. Arvind.

DR. NARAYANAN: I want to follow up on Eric's point that operating systems are another point of providing a shield, so to speak, to the consumer that should not be ignored. We have been talking a lot about

Web browsers, but operating systems are equally important.

One good example of this is news that came out just a couple of days ago of Ubuntu making a surge deal with Yahoo!, the default Firefox browser on Ubuntu is now going to tie into Yahoo! search rather than Google search.

The reason I bring that up is here we see that the operating system has the final point of control over what reaches the consumer, even though Firefox defaults to Google Ubuntu's able to change that to Yahoo!.

And this is also going to become even more important in the future, I think, because in the desktop space we have mostly had a near monopoly of Microsoft's operating system. Whereas, as more and more computing moves to phones, there the operating system market share is very, very diversified.

And so we are having this really complex set of partnerships and deals between OS manufacturers, and browser vendors, and search engine providers, and all of these different parties play a role.

MR. ECKERSLEY: That's correct. Thank you.

DR. NARAYANAN: Right. Right.

MS. HARRINGTON-McBRIDE: All right. With that I think it may be time to move to our final subject for this morning. And for that I will turn to Lori.

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

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

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

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

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

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

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

And I'm not sure that we have revisited how we ensure that that chain of accountability is actually achieved, and how you can ensure that when data flows to you that you understand where that data came from and the obligations that come with that data, and vice-versa when data flows out.

And it really becomes more and more important from the discussion we had earlier, which is bits and pieces of information as they get reconnected, or connected, become meaningful. And I think that we really have to think about how this networked environment that we are in really changes that concept of a chain of accountability that isn't so much a primary and secondary relationship like it used to be in the old days.

MS. GARRISON: Now when you implement such a program in a large organization, what is involved there? Is it a major rearchitecting of the system, or is this something that at this stage of the development can actually be implemented relatively -- and I'm going to use the word "easily," but it's not going to be easy.

But also because we have had some questions about this tension between regulating and having industry be creative, is it going to hamper or constrain innovation? How do you see this playing out?

MR. TAYLOR: I absolutely believe that if we don't have a mechanism to build out that chain of accountability, we run the risk over time for organizations that are really trying to do the right thing of it stifling innovation, and that's mainly going to come out of a reticence risk.

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

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

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

MS. HARRINGTON-McBRIDE: Pam.

MS. DIXON: I think one of the issues -- I appreciate your point, and I think I've thought about those a lot -- but one of the real down sides of this -- it's kind of like identity theft. Identity theft was a real boon to the privacy argument, but the downside of identity theft is all of a sudden you get all of these really invasive authentication techniques.

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

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

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

PROFESSOR HOOFNAGLE: Some of that -- I think some of the legal infrastructure is already there. So for a long time in the offline and increasingly in the online world major list houses have used contract to promote accountability. And if you get any of those contracts you'll see that they are -- they often follow fair information practices.

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

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

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

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

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

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

MR. TAYLOR: No. I just wanted to comment that I don't disagree with Pam that the concept I came up with is not a simple thing to implement. The point is that as -- if data is -- is flowing the way that we know it is from all the examples we have talked about, I think that the tensions here is the stifling of innovation if we don't have mechanisms to understand how data can be used and how consumers want their data to be used or not.

And so I think we have to come up with some way. Somehow, network affiliate advertising groups can figure out how to flow a lot of information with data for purposes to ad value of targeting information to consumers. I think there are mechanisms and technologies and ways for us to think about how we can ensure that appropriate information and obligations flow with data in the future.

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

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

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

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

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

MS. GARRISON: Eric, you had a comment?

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

I mean I don't even understand how to frame that discussion in an intelligent way. It points, in my mind, to the need to really think about how the consumers can control their own experiences when the data comes back to them. In other words, I don't care so much about if people are sharing my email address among all of them if I never see the email that comes from it.

So in the end it really puts pressure when we talk about the data flows through this complex web of interactions on the supply side, into what consumers can do to actually manage their desktop when they -- from the results of that data flow.

MS. GARRISON: Sid.

MR. STAMM: I just want to provide a technical data point. There is a group at the University of Wollongong who a few years ago did a study called Sit DRM, which basically applies digital rights management techniques to privacy preserving of data within one organization.

So it is a theoretical system, but I am sure that there is a variety of research out there who use similar technologies that say what the users' data can be used for and how it can be used, and then enforce it. I don't know how -- how it would work in practice, but it's out there.

MS. GARRISON: Eric, I think this plays into your trusted intermediaries concept, something that you feel strongly about in terms of addressing these issues?

PROFESSOR GOLDMAN: Yes. I mean the difficulty I have with some of the way the discussion has proceeded on this panel is that we are trying to put genies back in the bottle, I think is the metaphor that's been overused and in the end, ultimately, let's start with some premises.

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

What that means in practice then is that they have to defer to somebody else to do some of the management of their systems for them. You know, Arvind gave the example that we defer a lot of trust to our operating system. We have no idea what deals the operating system has cut upstream from us, but we defer the trust to them.

And we need to be able to either, from a regulatory standpoint, ensure that that is trustworthy, or we need to make sure the market mechanisms are strong enough that the technology, the provider's brand, will be sufficiently punished if they cut a bad deal.

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

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

MS. GARRISON: Arvind.

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

So I think it boils down to a question of incentives. Genetic data is viewed by consumers as very, very sensitive information and, therefore, this company felt that the proper thing to do was to have this reauthorization mechanism. So I think there is a role for very strong controls on where data is flowing.

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

MS. GARRISON: Pam.

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

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

MS. GARRISON: Well, I think we have come to the end of our discussion. I want to simply close with saying that we have the Chief Privacy Officer of Adobe who is attending today, and because we did talk about Flash cookies in the beginning, to announce that Adobe has filed a comment which should be up on our Website either later today or tomorrow, which will discuss in more detail how Adobe Flash cookies work, and also more information about the new 10.1 version that was just released.

I also want to thank each and every one of our panelists for a very stimulating and interesting conversation. So stay tuned. Are we going to have trusted intermediaries, as Eric suggests, so everyone is going to go out and hire some individual or company or entity to manage their identity for them?

Or are we going to do what Scott suggests and have some at least baseline industry standards that everybody agrees to and that are enforceable through an accountability mechanism? Or is it some merging of the two? And we'll discuss more of that as these roundtables proceed. Thank you all.

(Applause.)

MS. GARRISON: We will have a 15-minute break and we'll start promptly at 11:00.

MS. HARRINGTON-McBRIDE: 11:00.

MS. GARRISON: Eleven o'clock. Thank you.

(Recess taken from 10:45 a.m. until 11:04 a.m.)

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

MR. MAGEE: Good morning, everyone. My name is Peder Magee, and with me is my Comoderator Michelle Rosenthal. This panel relates to the Privacy Implications of Social Networking Sites and other Platforms.

I'm going to introduce our esteemed panelists and then we'll dive right into the questions. Going from my end to the other, we have:

Lillie Coney, who is the Associate Director at EPIC;

Chris Conley, who is the Technology and Civil Liberties Fellow at the ACLU of Northern California;

Ian Costello, Vice President for Product Development at LivingSocial;

Erika Rottenberg, who is the Vice President, General Counsel and Secretary at LinkedIn;

Tim Sparapani, who is the Director of Public Policy at Facebook;

Nicole Wong, who is the Vice President and deputy General Counsel at Google; and

Dennis Yu, who is the CEO at BlitzLocal.

Before we start, just a quick reminder that this is an interactive discussion. We will be asking questions of the panelists. We encourage everybody to participate. If you'd like to be recognized, please turn your table tent to the side.

MS. ROSENTHAL: I'll just remind everyone that if you
have questions, you should have question cards in your folders. Someone will be walking around to collect them, and if you are watching online you can submit questions to PrivacyRoundtable -- that's one word -- @FTC.gov.

Also, we have been told that a few people had issues with the Webcast. If you do have issues I'm told you just need to reload the Webcast and it should be working properly.

MR. MAGEE: Okay. Social-networking sites and related services have become a global phenomenon attracting hundreds of millions of users. Consumers use this medium to manage an online identity or profile, create and maintain a vast array of different personal and professional relationships or connections and traverse their social network.

I'd like to start the discussion this morning by asking why this medium is so popular, and what are the benefits to consumers who use social-networking sites. Perhaps Tim from Facebook can kick things off for us.

MR. SPARAPANI: Thank you, Peder. And thank you to the FTC for the invitation to come and address all of you and share in this conversation.

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

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

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

And that will continue to lead to a myriad of new value propositions which have not yet even been conceived of by people in this room, as smart as the people in this room are.

MR. MAGEE: Erika.

MS. ROTTENBERG: I echo precisely what Tim said and thank you very much for the opportunity to speak. What I'd say is that since Adam and Eve, people have wanted to connect. And you go back to the schtettles of Europe, and people connected within their schtettle.

You think about the Model T Ford. And people expanded their reach and started to connect with people who live a little bit further away. I used to live in Alaska and there are villages that were snowed in. And what did people do?

They used what was called RapNet, which is, you know, the old, you know, basically radio show. And you would call in to be able to do communications with people who lived in villages that were shut off because of the ice and the snow fields.

And what entities like Facebook and LinkedIn have provided is a way for people to connect to whom it is that they want to. With respect to LinkedIn, we believe and our user base believes that there is very, very compelling benefits to connecting.

Rather than if you think back to many, many years ago, you could send your résumé to one person, but what LinkedIn allows people to do and what people are clamoring to do is to create, in LinkedIn's case, an online professional identity that broadcasts to those whom that individual user makes a conscious decision to whom it is they want to broadcast that to, whether it's just to their connections, whether it's their connections of their connections, or whether it's to the LinkedIn community at large.

We look at, and our mission statement is, to connect the world's professionals to make them more productive and successful. The number of emails that we receive on a daily basis about, "I love LinkedIn"; "I got my job from LinkedIn"; "I got a new client from LinkedIn"; "I created a new business from LinkedIn and the connections."

We have also in a very, very broad scale -- and we do believe that we are changing the way that the world works -- we are creating economic opportunity, regardless of where it is that you live. If it's in, you know, the -- the connected Silicon Valley, the connected capital of the world, or if it's in a village in Nairobi, Kenya, it truly is creating an economic opportunity that levels the playing field and allows the advancement and enables the advancement of a global economy.

MR. MAGEE: Nicole.

MS. WONG: Thanks to Peder and Michelle who did such a great job of organizing this panel and for coming to California and bringing us sun for the first time in two weeks. So thank you for that.

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

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

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

The Google moderator basically takes in questions and then users vote about what, was that a good question, you know, like let's ask that one for sure. And what we got as of -- I checked -- midnight last night, we had 287,000 votes on over 7,000 questions from almost 30,000 people.

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

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

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

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

MR. COSTELLO: I think, kind of tying into what's been said, that with all this hyper connectivity people also not want to just connect, but try new things. People are really drawn to innovation, and with opening up these platforms and creating very, very low barriers to this innovation, it just continues to give people new things to try.

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

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

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

Things like photo and video sharing, there is lots of sharing of information online, and it might be helpful to consider sort of how this space offers from the offline space and whether it differs from the offline space. Lots of personal data is being uploaded every day and great numbers of people are able to access that data.

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

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

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

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

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

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

We have Bozeman, Montana, that had a job application that required applicants to provide their logon and password for social-networking sites, and what they said was basically for background check purposes. We have had circumstances where the researchers at Carnegie Sci Lab who looked at social security numbers and the master death records and basically proved that the information provided by social network users, the basic logon information, name, location of birth, date of birth, they could use that information to literally guess the last four digits of individuals' social security numbers, which are very relevant for identity theft, which is one of the issues regarding how social-networking services provide content to other users.

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

MS. ROSENTHAL: Thanks, Lillie.

Chris.

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

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

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

The MIT research project is called Gaydar, and essentially all it did was look at the social graphs of who your friends were. It looked at their gender and their sexual orientation and it tried to figure out, well, from that can you figure out this person's likely sexual orientation.

So this is not photos. This is not like content as we think of it, this is just very, you know, basic information that suddenly exposes a lot more about people than they might expect. So this is really changing in a way that, you know, all the facts about data being portable and accessible and aggregable makes the social-networking world a lot different than the socializing that we are used to in the real world.

MS. ROSENTHAL: Thanks, Chris.

So some academics have noted that minors are at a greater risk with respect to social-networking sites. And the idea is that, you know, minors don't think about the long-term consequences. They only think about the short-term benefits. So are minors at a greater risk in this space? You know, is this something that we should be concerned about? Do they -- are there other things that we should be worried about that maybe don't apply to adults?

Lillie?

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

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

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

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

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

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

MS. ROSENTHAL: Thanks, Lillie.

Anyone else? Oh, Nicole.

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

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

And so the answer is about education and modeling well and teaching anything -- and here's the vulnerability I think for kids. It's about judgment, right. Have we taught them to exercise the right level of judgment about their privacy or who they friend or don't friend or upload to a particular service.

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

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

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

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

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

MS. ROTTENBERG: Just a real quick comment. I don't disagree with what's been said, and what I would say is that for every benefit in the world there are some down sides or there will be abuses. And you know people pick -- for a future employer to request a user name and password, I mean people shouldn't be exposing their user names and passwords.

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

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

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

You can't expect the children or their parents or for the consumer to be able to have the same weight and voice in the environment where a lot of data collection is happening.

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

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

MR. MAGEE: That's a good point. So we have talked about some of the benefits that we see and some of the challenges and risks of potential harm, as well. What I'd like to focus on for a little bit is the idea of unexpected sharing, that seems to be where a lot of the potential problems come from, and talk about the dichotomy between the expected and unexpected sharing.

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

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

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

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

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

So if, for example, on your social-networking profile I did this, just to see, right, I changed my preference to, you know, male seeking male, and I saw I was flooded with a lot of, you know, male seeking male ads. Or I changed my religious preference to say that I was Jewish, and I saw all these Jewish ads, right.

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

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

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

MR. MAGEE: Well, so what are some ideas for perhaps narrowing this gap between the consumers' expectations and their actual experience? For instance, could we set certain controls that restrict the user's ability to share information for a certain period of time before -- after which they are familiar with the settings and the privacy controls?

Tim?

MR. SPARAPANI: I was going to say Facebook has a fundamental philosophy, which I think is important to be recognized and vocalized, which is that we trust our users. We believe there are smart people out there and we believe that if we give them tools to control their information and give them full knowledge and information that they will make choices which reflect their own values and attitudes.

And we have seen the people fall along an entire spectrum of attitudes about privacy from people who would share everything with the world -- that's something I would never do -- to people who would share nothing with the world and would rather sit back and watch other people's experiences or not participate at all.

And I think it's important to recognize that when we are talking about particularly free services that we give real control to people, as we do at Facebook and

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

We should give them the information that they need. We should help them understand what the possible implications are and then we should get out of the way. I think that's where innovation is important. We can't be in a position of trying to control people's attitudes, particularly when we are talking about a free service, a voluntary service.

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

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

And there has been a lot written about, boy, people sure aren't going to understand what's going to happen, and people are really going to be confused about that. A lot of people speculated and they worried aloud about it. I did, frankly. I spent a lot of time thinking about it with the teams that I was working with within Facebook before this happened.

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

And we found something extraordinary. We had almost 35 percent of our users who actually customized their settings. They actually customized and they took control of their data, perhaps for their first time. Thirty-five percent of 350 million users is an extraordinary number.

And what we found out is that we found that at least a third of our users were also making active choices through this process. So what we saw is there was actual knowledge, an actual choice being made by our users because they are smart. And when you give them information and tell them what the consequences are, they make the right choices. And I think that's what we saw, and we are pretty excited about it.

MR. MAGEE: Chris.

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

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

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

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

So when we are thinking about defaults, you have to think about, well, what are the risks, what are the harms if people over-share. What are the costs? Will people, if they really want to share things, find ways to do them?

Will people realize they are not sharing more easily than they realize they are sharing? When you are thinking of default and how they match with user expectations, that's one way of meshing those two together. Not the only, but...

MR. MAGEE: Erika.

MS. ROTTENBERG: Yes. I would also go back to -- the question was framed in terms of what are unexpected sharing and helping you prevent that. So, first and foremost, is education, I believe, and that goes on the online setting -- well, it is the village and it's all of our responsibilities collectively.

As a platform we can provide clear disclosures, and it's important to have clear disclosures. Full transparency, say what it is that you are going to do. Do what it is that you say you are going to do. Give the users choices. Give the users controls.

I mean I think Facebook has set a great standard in terms of granular controls. Following up on what you have said, default settings. Now I know that we at LinkedIn take great pains, as I'm sure, my colleagues do in terms of what is it that we think most of our users want. You are absolutely right.

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

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

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

If we were to breach that trust, if we were to mis-use information, if we were to suddenly sell user data when we tell people that we don't sell user data, we can breach that trust in a heartbeat. And our interests are aligned with our users, because if we breach that trust, our ecosystem will fall apart.

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

Nicole.

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

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

When I and my team sit down with our engineers here the things we go through. The first one is is there value for this product for our user, because that's always got to be the thing that leads. The second is can we build in the best possible privacy standards into that product, whatever that might be, whether it's health or social or search.

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

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

Users are more sophisticated than that and they want to be able to say things like, I want to share with only this set of people, but not that set of people, and it's our job, as smart as our users might be, it is our job to build those controls for them.

And the final one is to be responsible stewards of that information and to do the things that our users expect of us in terms of keeping their information secure. I thought it was interesting, Peder, what you were raising, which is should you give users kind of like the training wheel period of figuring out the UI before you like set them free with it.

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

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

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

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

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

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

I agree with Tim and Nicole that if you trust the users, they will be able to figure it out. There are self-regulating mechanisms. For example, in an ad or inside an app you can actually rate it, and we have worked with Facebook on certain ads that are bad where there are more people that click the x saying it's misleading than the people actually click on the ad.

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

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

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

MS. ROSENTHAL: Okay. Lillie, we are going to get to you in a second, but maybe you can just frame the third-party app discussion a little bit and talk about how these third-party apps are monetized and sort of how the businesses are run. We know there is a big difference between the -- we talked a little bit about the barriers.

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

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

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

And Facebook, MySpace, it's not so much with LinkedIn, but you are going to see these kinds of ads that will try to say, you know, give me your cell phone, install this toolbar or sign up for this particular offer. We have seen a lot of the advertising -- this was -- not anymore, but this was a couple years ago just when we were all working together to try to figure out what to do, a lot of noncommerce related items, right, because people weren't on a social network site to check out, to put in their credit card, right.

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

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

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

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

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

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

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

They bring new opportunities that consumers have never had before. So that should be recognized, but there are in fact some bad actors. We have people who regularly or occasionally violate our clear terms of service that developers are supposed to abide by.

What's exciting about our system and what we think has been a really neat privacy innovation that we hope others will follow is that we have on our site an ubiquitous ability to report an application which does not meet your expectations as a consumer.

We literally have taken a crowd sourcing approach to the policing of these applications. So when consumers have an experience which does not comport with what they thought was going to happen, they tell us and then we begin to take action, and that can be everything from just calling somebody up on the phone and saying, what is going on; it looks -- you are taking data you told us you weren't going to take; please quit doing that and send back the data, all the way up to cease and desist orders. And so we have to act as a police person and we do.

MS. ROSENTHAL: So okay. So you do. Facebook has lots of employees.

What about some of the smaller social-networking sites, really? Should we be concerned that not every social-networking site has the tools to try to police these third-party apps?

MS. CONEY: I think that there are problems with third-party applications because they are not as transparent. Consumers don't understand them and as far as regulation controlling what they do or what they can do with data they collect, or whether they ought to be allowed to collect information on consumers, all of that information is -- those questions haven't been really resolved.

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

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

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

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

MR. SPARAPANI: This problem, such as it is, is relative in scope to the size of the advantages which are created by applications. It's a small problem, as Dennis I think was making clear. Yet nevertheless this is where our economy is going. If you ask people in the valley, this is where the energy is.

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

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

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

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

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

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

MS. ROSENTHAL: Well, yes. Ian, do you have any -- your company obviously collects information through the use of platforms through the iPhone, I believe, and also on Facebook.

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

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

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

MR. COSTELLO: Yes. Again, I kind of referenced that as the lifeblood. One of the examples we have, one of our apps is pick your five, where it's basically pick five things and you can pick five anything, and I can pick five places that I've lived or my five favorite TV shows or my five favorite movies and share them with my friends.

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

MS. ROSENTHAL: Okay. Thank you.

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

MR. CONLEY: Well, I'm going to start by talking a little bit about the application we wrote. So we look at Facebook and not to pick on Facebook, just because they were the one we were focused on at the time, and I learned six months ago maybe that how much access Facebook applications have to information just by default, if you run an application.

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

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

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

You can be, or you can be someone who hasn't written a program in about seven years and wants to dust off some skills and see what he can come up with in a couple of days. And so we wrote a little quiz of our own that's basically is a quiz about how much do you know about how applications access information.

And if you take the quiz, and probably some have, some haven't, you can find out that if you run a quiz, whatever the question is, the quiz can still see your pictures. It can see your religion. It can see your friends' lists. It can see your groups.

It can also see, for any of your friends who haven't changed their default settings, their profile pictures, their events, their political preferences, their personal information of all sorts. And to counter Tim, I mean I think of myself as an educated user, but maybe I'm wrong.

I actually got to demonstrate this for a group of Electronic Frontier Foundation interns, and I think the greatest compliment I've gotten is that they were all scared when they went home, because this was -- these are people who know technology and they are not really familiar with how these applications work and what goes on behind the scenes.

So we obviously have a long ways to go to educate the consumers. And when we talked -- we released this to the public we actually had more than a few people. I couldn't bring them all here, so I just brought a printout of some of the names of people who signed a petition asking for more privacy.

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

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

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

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

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

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

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

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

And I'm wondering to what extent social-networking sites, other platforms, are competing on privacy and whether there is a realistic chance that, say, a consumer who's devoted a fair amount of time and energy into creating a profile and creating a list of contacts would simply pick up and move to another, similar site that perhaps has a little bit of -- a better privacy practice than the former.

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

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

Users could say, I want to, you know, delete my data and we will delete data. I mean there really is, you know, trust that is placed there, and I think that if we abuse that then people will leave. I mean I will tell you that the in the DNA of our company there is kind of a slogan that goes around, but it's very, very serious.

It's not what we -- the comment is, "It's not what we do to our users, but it's what we do for our users," and trust is in the DNA of our company with respect to each product release or feature release that we put out there.

MR. MAGEE: Nicole.

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

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

And what they did is they basically took a page from what we had done when we launched Gmail in 2004. When Gmail launched and we were at that time entering the space of Webmail, so Yahoo! and Hotmail were way out ahead of us, and we wanted people to try us.

So what we did was say, come try Gmail. If you don't like it, we have built portability in. You can move all your emails. You do not have to shuffle them over one by one; all of them easily to the next service if you decide you don't like us. Well, our engineers last year decided we should do that for every service.

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

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

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

And most times users, when they come to a new service, don't think about how am I going to end this relationship if I don't like it in three months or a year? What are my options at that point? What our engineer said is, you should be able to end that relationship. You should be able to move your data, move it freely, like as in it won't cost you any money and it shouldn't take you a lot of time. And that was one of our priorities.

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

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

MS. WONG: Yes. So the contacts lists I think are different and I'd have to go back and look at the specific feature for contact lists. The emails, right, it’s literally, like, take all the email content that you have and put them in a different container and the features that we are talking about are typically like the documents, the calendar, in which case these are, you know, it's like your home calendar now, right?

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

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

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

There are dozens of competitors around the world that we have, and there will be more, I am sure. So we intend to distinguish ourselves through privacy, and I think you have seen that our model has been one to look at the fact that there are not harmonized laws between the U.S., Canada, Australia, and Europe, and we have tried to say, given the impasse, we are going to do something different.

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

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

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

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

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

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

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

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

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

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

MS. ROSENTHAL: Do you have any audience questions?

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

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

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

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

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

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

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

MR. MAGEE: Chris.

MR. CONLEY: There is more than one type of data. There is the user-created data, the picture that you upload. There is the time stamp that records that you uploaded a picture and here's it with its name. There are the people who clicked on this picture and the people whose pictures you have clicked on.

There is also secondary data and there is a question about that, about whether when you delete a profile does that also delete, insofar as possible -- you can't practically erase every trace of everyone -- but are there efforts made to delete all the other records that identify this person was a Facebook user, or Niceface user or LinkedIn user or whatever the case may be.

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

Although you can leave, there is no where you -- there is no other place in the universe you can actually go and experience that life or the applications that you have. So that's one issue. Even if you say people can download this to their desktop or their personal computing device, that may not really be a choice.

So making sure that when we talk about consumers having this ability to go somewhere else, that isn't in fact a truthful statement because of the size and the variety of the applications that are out there.

MS. ROSENTHAL: Thank you.

So I'm going to switch gears a little bit and get back to consumer control just a bit. We don't have much time left. So we are going to try to get a lot in.

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

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

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

Anyone? Tim -- or Erika.

MR. SPARAPANI: No, please.

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

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

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

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

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

MS. ROSENTHAL: Thanks.

Chris.

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

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

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

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

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

MR. SPARAPANI: Yes, I need to respond to Chris' comments, because it's just actually not accurate what Chris said, and I'm forced to respond. It's always been the case on Facebook that if you were a fan of a particular organization or cause, you know, believe me, I used to be at the ACLU and people would consider that sensitive and damning in some places.

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

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

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

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

MR. CONLEY: Ten seconds.

MS. ROSENTHAL: Yes. Yes.

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

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

MS. ROSENTHAL: Erika.

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

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

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

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

Who do you want that to go to? And you can decide that on a granular basis. We recently announced a Twitter integration, and you can choose if you want to have a network update be tweeted out to all of your Twitter connections at the moment that you are doing it, or you can choose no, I don't want that to go out.

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

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

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

This is an open question. Lillie.

MS. CONEY: I'd be happy --

MR. MAGEE: I thought you might weigh in.

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

MS. ROSENTHAL: And we appreciate that.

MS. CONEY: And I know you do. You know it's with deep felt, heartfelt commitment that we send in complaints and draw the agency's attention literally in the best, effective way we know how to identify issues where consumers are being harmed. This agency is the agency. It's the backstop for helping consumers.

We like the ecological approach that when there is an effect in the environment we respond. We don't let things overwhelm the system.

MR. MAGEE: So what would that mean --

MS. CONEY: Yes.

MR. MAGEE: -- for the FTC?

MS. CONEY: It means that, one, the FTC has the authority and the ability to act, and we want to see them do that. We are looking at what's happening in Canada and in the EU regarding social networking. Their data protection authority is stepping in there and establishing new norms, or new rules, or new policy or regulation that, in effect, extend consumer protection to U.S. residents, because the Internet is a global medium. So we do want to encourage that, and we will continue to encourage the Agency to do that, as well as those who are making legislative proposals.

MR. MAGEE: Chris, do we need government intervention in this space to establish privacy norms?

MR. CONLEY: Well, I think one of the issues is that one of the market failures, of course, comes from a lack of information. So one of the ways that government regulation could help is to encourage more transparency around how often is information disclosed to third parties through search warrants, or court orders, or whatever it might be.

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

And if that's not coming, if the market itself isn't generating that information, that might be a place for government regulatory agencies like say the FTC to get involved.

MR. MAGEE: Dennis, how about it? And what would be the impact if there were government intervention on innovation in this space?

MR. YU: I think it'd be a baby-and-the-bath-water situation because, from our perspective as an advertiser on behalf of major brands, as an agency, and also as an individual, I'd say that 99 percent of the privacy abuses are handled by market forces because, for example, within Facebook you can click on ads that are bad. You can report people who are sending you messages that are spammy, you know, and LinkedIn. You try to friend someone who you don't really know. There are a lot of ways that -- there are crowd-sourcing ways to fix these issues.

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

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

MR. MAGEE: Okay. Nobody wants that.

Nicole.

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

You have here some of the best players who have told you we compete on privacy. But as a regulatory agency you have the ability to go and find some of those other players who are not as transparent who are not going to compete, who are not working hard to do the right things by their users.

And I think that before any sort of regulation happens you need to do more fact-gathering in that space, which I don't even fully understand, right? The credible players are here to do the right thing. The folks who are in the shadows are the ones that I think, as a market we need more information about to effectively legislate.

MR. MAGEE: Anybody else?

MS. ROTTENBERG: It's obviously a very, very complicated question and a one-size-fits-all regulation or a one size -- regulation that's a one size fits all I think will fail. I mean, it's a very, very blunt object. Certainly, the FTC needs to be involved. Certainly, there are bad actors and where there is bad actors it's our collective responsibility, not just here but the collective responsibility, the village responsibility to shine a light on that.

Transparency is key, key, key, key. I think that there is -- that significant attention needs to be paid to what unintended consequences might be. I might lock my door by putting a chain on it. Does that mean that no one's going to come in? So I do believe that there needs to be significant fact-gathering.

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

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

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

(Applause.)

MS. ROSENTHAL: A quick announcement, quick announcement. This is obviously your lunch break. If you would like a list of restaurants in the area, there is one outside on the tables that you walked by when you came in. Feel free to pick that up. And we will be starting again at 1:00 -- or, I'm sorry -- 1:30.

(Luncheon recess was taken from 12:20 p.m. to

1:30 p.m.)

ASSISTANT DIRECTOR OLSEN: All right. Why don't we get started?

We're very pleased to have Danny Weitzner join us. Danny serves as the Associate Administrator for Policy at the U.S. Commerce Department's National Telecommunications and Information Administration. And TIA serves as the principal advisor to the President on Telecommunications and Information Policy.

He also was Cofounder and Deputy Director of the Center for Democracy and Technology and Deputy Policy Director for the Electronic Frontier Foundation. We're fortunate to have him here today and look forward to his remarks.

(Applause.)

REMARKS

ASSOCIATE ADMINISTRATOR WEITZNER: Thanks very much, Chris.

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

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

So as a member of the Obama Administration I'm really pleased to have the Commission as a partner in our efforts. I think since I'm far enough from Washington that I can say as a citizen I'm happy that you are out there protecting me individually.

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

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

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

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

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

But we shouldn't, at this moment, think that we somehow understand the whole environment, that the innovation is slowing down or stopping, or that we would want that to happen. I think that we have a whole new array of innovative new services, whether they're mobile services, location-based services, services that take advantage of tremendously-increased powers of data aggregation and data integration that the Web makes possible. So we have a whole -- a continued stream of innovation.

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

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

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

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

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

And I think that in a certain sense in the year 2010 we're entering what you could think of as the third phase or the third decade of internet policymaking. The first phase was really exciting. A number of people in this room were around for that. And the internet was this cool new thing. It was transitioning from a kind of a plaything in the research and education environment. It was happening out in the proverbial garages here in this part of the country.

And the attitude, the policy attitude that the United States took to the internet was a very simple kind of hands-off, more-is-better, let-it-all-happen, a deregulatory approach. And by all accounts that worked pretty well. We had a period of extraordinary growth. We had tremendous global leadership in this environment.

But I think that in what I think of as the second phase of internet policymaking, as all this cool technology and these cool capabilities became part of people's daily lives, really in this kind of transition of the internet to main street I think that we had the beginning of some simmering tensions. I think we see very clearly increasing worries on the part of consumers and citizens about what their privacy rights were in this environment.

Again, I think that the efforts that the Commission and the U.S. Congress took helped to address some of these concerns. But I don't think that the job is all done there. As we enter this period of time in this kind of second decade of internet policymaking, you have 70 percent of U.S. households, just about, are on the internet. So it's become clearly an essential resource for our country, for the world. But, as I said, I think there are real tensions that are developing, tensions in the privacy-policy arena, tensions in other arenas as well. The online-copyright-enforcement arena and cyber-security arena.

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

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

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

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

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

I think that questions that we see raised on panels earlier today, questions that are floating around in the private sector and in academic discussions about enhanced roles for governing usage of data as opposed to or in addition to rules governing collection of data I think are very promising directions that deserve to be explored.

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

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

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

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

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

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

(Applause.)

PANEL 3: PRIVACY IMPLICATIONS OF CLOUD COMPUTING

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

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

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

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

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

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

So the groundrules for this Panel are the same as for previous panels. Panelists, if you have a comment, please raise your table tent on its side. We hope to keep this very lively. And this is not a shy group, so I have no concerns that people will chime in as much as possible.

For audience members who have questions, we have comment cards, so you can write your question on the comment card. It will be brought up. And for those of you following on the Webcast you can email your questions to PrivacyRoundtable@FTC.gov

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

Lindsey Finch from Salesforce.com;

Beth Givens from Privacy Rights Clearinghouse;

Nichole Ozer from the ACLU of Northern California;

Harriet Pearson from IBM.;

Paul Schwartz from U.C. Berkeley; and

Scott Shipman from eBay.

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

So, to start off, I'd like to start with the discussion of what's new about this model. Because really we are talking about a form of outsourcing here. So let's talk a little bit about how this particular business model is different from other types of outsource services that have been happening for years. And I like to start with Harriet.

MS. PEARSON: Thank you, Katie. And thank you to the Commission for having this discussion.

So rather than call it a business model, let me offer the thought that cloud computing is really a computing model. And the notion here that we're talking about probably 50 or 60 years worth of modern IT industry history, you've only had basically three different computing models in existence. And so the fact that cloud is a new one is rather a big deal because every prior wave has created a rush of innovation and change in organizations around the world.

And the first model, I think just to give a little bit of historical perspective, was really kind of the original, very centralized batch processing characterized by the mainframe era. That's '50s, '60s, '70s. That was the era. And actually notably, from a privacy-policy perspective, that was the era in which some of the seminal work that still informs our work on privacy, was done. 1973, the Fair Information Practice Principles coming out of the HEW Task Force and other seminal work really was characterized and informed by the computing model of that day, which was very batch process, few users, lots of controls, kind of slow, and limited in its distribution.

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

Fast-forward again and what Danny Weitzner talked about, the internet and he came into policy in the '90s, and so did a lot of -- so did I, at least -- a lot of us here. And I would say that was the start of a dialogue that we are continuing this day. That's the emergence of what we now have put a name on. We put a name on it called cloud computing. But I would submit that with the emergence of the Web and the ability then to dynamically access and share information and distribute computing, what we're seeing today is really the next step, the evolution of that.

And I am borrowing an analogy here from a colleague of mine at IBM who talks about walking in a forest. And you know how you walk in a forest sometimes and the trees start changing because you're changing altitude, you're changing location. And I think we started walking in that forest in the '90s and the trees were changing. And we were talking about the Web and cookies, and it was sort of simple. We took some initial steps to support innovation and growth in that area. But at this point I think a lot of the trees have changed and we are in a very mature area where organizations are looking at this computing model and saying: We're taking advantage of it.

So I would submit that the privacy issues, per se, are not new. We have been working on them as enterprises. I know our company has for, I would say, a couple of decades. But the issues are the same. They are the issues of which jurisdiction applies when you actually collect and compute; instead of having batch and localized processing, if you had distributed and network processing, jurisdiction matters. Cross-border issues of course are a part of that. I think data security is part of that: Who has access, who has the ability to see the information. What do you do when you need to port over.

You know Nicole Wong talked about it from a Google perspective, from an end-user perspective. When you think about an enterprise setting, what are the rules of the road and how do organizations come to agreements about what the rules of the road should be.

Data minimization is another. And kind of rethinking, and just to turn it over to somebody else so I don't talk too much, because that's the rules of the panel, just the thought is if the computing model of the '60s and '70s really informed our thinking and our policy models, what does the computing model of this era due to inform the policy models of today?

Networked, fast, fluid, all of us are creators of content. A lot of us are analyzers of content. Very international distributed. What will it do? And I think we're poised now, as Danny said and others have said, and to rethink, without disposing of the values of the past or the good work of the past, to rethink how we support innovation and do provide that stability and certainty that is necessary for economies to grow.

MS. RATTE: Thank you, Harriet. That was an excellent introduction.

And I think we'll delve into some of the jurisdictional issues that you raised with respect to cross-border data flows later on in the panel.

Lindsey?

MS. FINCH: I just wanted to add to I agree with everything Harriet said. And when we talk about B2B cloud computing as a type of outsourcing, I would actually argue that when two companies are engaged, when you have a business customer and cloud computing customer, it's actually a much more participatory form of outsourcing than traditional business-process outsourcing, where an entire function is being handed to an outsourced company.

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

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

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

Beth, did you want to...

MS. GIVENS: Well, we keep track of data

breaches on our Website. And certainly that is an incentive to not keep a lot of sensitive data, especially Social Security numbers. It's very, very expensive for companies to have to respond to a security breach. If they just hadn't held onto the Social Security number after they determined they didn't need it, they wouldn't be involved in the very expensive lengthy and also, in terms of reputation, bad experience of hanging out your laundry, and saying, 'Whoops, we had a security breach and now we have to tell you all about it.'

MS. RATTE: And are we also moving in -- do we need to think about questions like is there an incentive to monetize all of this data that's lying around? Whatever the rules are today, the longer you store the data, the more data you have. There's the incentive out there.

Harriet?

MS. PEARSON: I was actually going to talk about the prior issue, just the minimization and storage costs. It's true I think in an abstract, stand-alone sense that the price of storage is decreasing and you can only, as a consumer, look at some of the free email accounts to realize that. But I think in an enterprise context, as Beth said, the policies that have emerged in the last decade or so do put some pressure on an organization, whether it's because of ediscovery or its data breach or other obligations or risks, to try to have better data hygiene. I don't think we can say that we are all the way there. Actually, I don't think organizations are yet. But I think that's a trend that is countervailing to the notion that storage is free, therefore there will be a proliferation. And it's one to watch. I don't know exactly how fast it will develop, but I see it happening in the marketplace.

MS. RATTE: Scott.

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

That argument is the same argument that we've heard in the fraud or the analytical-forensics spaces where a scientist in a fraud-research area will say, 'You know I don't know if that data will help me find a bad pattern, someone doing something illegal. But I won't know unless I have the ability to analyze that data.'

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

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

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

MS. FINCH: Sure. From a business perspective it comes down to what our customers demand and what the regulations require. And some tools that are currently being offered are things that allow customers to look and see when data that they have input into a cloud service was input, when it was last modified. And, using those tools, you can determine what data might be ripe for deletion.

But ultimately it's up to the customer, the business customer, that is, of the cloud service to determine when that data is ripe for deletion and to actually delete that data, because they're in control. To use the European terms, they would be the data controller in that circumstance.

MS. PEARSON: There is a suite of, it's kind of a field, there's a field that we kind of coined the privacy profession in the '90s that is evolving. And I think my own observation of how those of us who are involved in privacy from an enterprise point of view, how do you make it real, how could you make it come to life, are more and more working on data-governance, information-governance type activities. It's kind of a growth area. And we intersect with a lot of other fields and areas where you need to optimize data.

And, so to Lindsey's point, there is a whole suite of technologies and capabilities around data discovery, data classification that allow you more to automate the location and the management of information.

And that certainly helps in that trajectory to get better hygiene. I'd say they're still kind of the in the early stages of that.

MS. BERGER: Yes. In some ways we can talk about this whole idea of default settings. If storage is cheap and time has become your capital, are you going to invest the time to perform even minimal hygiene? What can be done to encourage companies to do this better?

PROFESSOR SCHWARTZ: If I can kind of speak to this initially, that question, almost as a law professor and a little bit more abstractly, I would start off by saying by actually drawing on a report that I did for Richard Purcell in the Privacy Projects where we looked at six leading North American companies and tried to figure out what they were doing in terms of global data flows. And we found that there were three things happening.

There was an enormous change in scale, there was a change in the type of processing, and there was also a change in management. And so the change in scale meant that you were going from batch processing, occasional processing, to continuous events and continuous processing and happening automatically, rather than having someone decide transfer by transfer, but a computerized process.

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

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

And so the at least kind of like law professor answer to your question would be: Figure out a mixture of carrots and sticks so that you kind of do the Marty thing, where you are encouraging the set of companies that aren't in the good room to go there, but by doing that you'll be incentivizing the companies that are investing in privacy protections to continue to do so, because companies are not just like black boxes. There are people who are fighting for budgets and fighting to be able to convince their bosses that really we should be making this decision. So that would be my answer for that: Carrots and sticks.

MS. BERGER: How would we achieve some sort of transparency as to who is in the good room and who is in the bad room? Would this involve audits of retention practices that are being carried out or what would we need to make this effective?

Lindsey, do you want to take a shot?

MS. FINCH: I think transparency is key here. It's very challenging in the B2B space for cloud providers to be transparent with consumers because we don't have a direct relationship with those consumers. But we do have public-basing Websites. We do have contracts with our customers. And I think that in terms of some self-regulation, in terms of best practices, I mean I think data ownership is a great example. When you enter into a contract with a cloud computing company, who owns that data, who has ownership rights in that? There can be standardization around that, and I think that's something that can be streamlined.

And then companies that utilize these cloud services need to be transparent with their end-consumers, the individual, so that they understand what the practices are.

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

MS. BERGER: Nicki.

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

And I think what's made possible all of this being able to trust companies and individuals with our information is that there has been this trust and there has been this ability to retain control even if you don't retain possession. And when ECPA was passed in 1986 maintaining this kind of control was on the minds of Congress.

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

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

I think, as Harriet said, a lot of this is not new, the issues of possession and control, but there are some things that are quite new. You know it's not a surprise to anyone in this room that the efficiency of copying and accessing and mining and sharing data has increased astronomically in the past 20 years and that the business models have also changed. There is an incentive for companies to look to access this data, to mine this data, to share this data, and I think those are important issues we need to think about because the information is going to one company who may then share it with another company who then might be subcontracting it to another company. And the original consumer likely doesn't know who those people are, what they're doing with it, what information they have, and what standards are being used to protect it. So you have got sort of layer upon layer of remoteness from the original consumer.

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

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

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

And the factual point is that a cloud is not a cloud is not a cloud. You have various ways to tap into virtualized, distributed computing, and all the other buzzwords, but basically there is this thing going on. The Web in the '90s and what we see as consumers made it possible to change how we communicate with one another and the kind of services that are provided.

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

So I think it is important to understand the variety of the computing possibilities here. And then you can apply the analysis that says: Okay, if you are, for argument's sake, a large financial services institution and you are doing a private cloud, I do not know that the issues are that different from a consumer perspective because you are still doing the same thing. You're just using a different back end. If you are a large organization or a small company and you are tapping into a public cloud, that may raise those issues.

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

MS. BERGER: Before we become too specialized in our discussion of the different context or types of cloud, can we talk about what is the role of transparency in the cloud? What about is something that consumers should be interested in knowing and what about is just going to be what another panelist called today too much information about information, or what I like to call privacy TMI?

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

Scott, do you want to start?

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

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

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

And the question I would ask is: Okay, by law they're required to provide that list, and we update that list ad nauseam. Right. I mean imagine every time we enter into a new agreement, we update our privacy policy in the appendix and we add another company to that list and the general or anticipated use that that provider can use the information for.

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

MS. BERGER: Yes.

MR. SHIPMAN: I pose that question because, I think as Harriet was saying with her last comment on policy, which is if we were to adopt more of a holistic, use-based approach, so that we knew generally the service providers can only use the information to facilitate the service from which they have been retained, then does the consumer have a broad -- have we increased their broad level of understanding of how their information can be used, so that they know that the responsible party to go to is in fact the controller or the entity that they have a direct relationship with.

MS. BERGER: Okay. So Scott's given us an example of a list of very concrete information that may not present consumers with any actionable data. It may just be a list that doesn't give consumers good options for the activity, but what is some information that would be good and would give consumers opportunities that they might use?

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

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

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

So I as a consumer, if I am doing business with one of you guys out there and I go to your privacy policy, this is the kind of general information that I get.

Also things like: 'Service providers may have access to your personal information for use for a limited time.' I have no idea for how long. 'But when this occurs we implement reasonable, contractual, and technical protections to limit their use of that information to helping us provide the service.'

So when I go to major companies and I read their privacy policies, I do not know who they are working with and I do not know what information is going to them and I do not know what the protections are. And even if I do know who these companies are, we did a lot of digging to try and find actually B2B contracts between companies and other companies. And some of the protections are not good, giving a lot of latitude to disclose information that's been given from one company, a primary company, to a cloud computing company sometimes with no notice to the initial company and certainly no notice to me as the consumer.

So we get really general language that, 'We reserve the right to disclose, sell, or license your content of data when we may determine it to be necessary or desirable.' Okay. Or things like, 'We may access or disclose your personal information, including the content of your communications.'

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

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

Paul, did you want to...

PROFESSOR SCHWARTZ: I think we have to think about why we want to inform the consumer and who the consumer is. And so if you want to move to, as Nicole has said, the right kind of B2B contract, that means you have a model of what that is. And it may be that kind of model has to come from legislation or the FTC. The difficulty is in just opening up the information to the consumer is that does not necessarily get you there. And I think there is a real issue with the TMI.

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

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

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

The final thing, Fred Cate has a great

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

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

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

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

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

Lindsey.

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

But for the moment I will assume that secondary use is a use of the information that a consumer would not necessarily expect when they hand that information over to the initial collector and user of that information. In the cloud it really varies contract to contract, provider to provider, and to really look and see. To the extent a company is acting as a service provider or, to use the European terms, the data processor rather than the data controller, then that entity should only be using the data as instructed by the data controller or their customer company.

And I would be looking for terms in a contract that say the data is only going to be used for those purposes. So you really need to look at how the information not only is going to be used but when the information can be accessed, when the information can be disclosed. So those would be some standard terms that I would be looking for in a B2B contract with a cloud provider, because it really depends on the model right now, but I think there is room for self-regulation here and possible enforcement if there is going to be uses of information that goes beyond what that contract is between the cloud computing provider and their customer, and then going back to that original notice that the business customer has given to consumers.

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

Thank you, Lindsey.

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

MS. BERGER: Yes.

MS. GIVENS: Well, to lead off from what Nicole said about fuzzy terms, and I guess I could even say cloudy terms, but the difficulty of figuring out what is going on in a privacy statement or a policy statement, there are many consumers who actually need to know the details of what is happening to their data as Company X hands it off to Company Y. In extreme cases there are stalking and domestic violence victims who will certainly want their address to be protected. They should also know that in a cloud environment there are lower legal standards for search and seizure. So there are issues like that I think it would be good for consumers, especially those with particular needs, to know about.

So Company X contracting with Company Y, I think Company X should tell the consumer and give them enough information about their dealings with these third parties that they could make informed decisions, that it would be good to know things about the company's stability, for example; access provisions, deletion provisions, how do you get your data out; customer service points of service, how do you complain; this is key, is the data encrypted because a lot of these issues go away if the data are encrypted; and, of course, the location, where is that data held.

MS. BERGER: Anybody else want to comment on things that consumers might have an interest in knowing about their data stored in the cloud? We've amassed quite a number of examples here.

Nicki and then Harriet.

MS. OZER: I guess one important thing for me would be to know what kind of data is going where. We are talking about companies collecting vast amounts of information about potentially who we are, where we go, who we know, our search, our book and video records, our health information. Some of this, this is vast amounts of information, some of it very sensitive to who we are.

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

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

MS. PEARSON: Let me try to take us back a little bit, though, because I think part of the discussion here, I don't have any disagreement, indeed I have a lot of support for the aspiration that we all should know, because with knowledge comes power, right? We all should know what is happening to information that relates to us. That is a good goal and aspiration.

But I guess I would put forward this notion of there are other goals as well and the goal of making sure that that information about me is not used to harm me, for example, is as perhaps an important of a goal or perhaps could be a priority goal that we might want to keep in mind as opposed to knowing for knowing's sake. And I just put it out there as a policy thought.

Let me also throw out an example, a concrete example of -- I think because when we are talking about information we are giving, I think we typically default to the online experience. And the last panel talked a lot about the social-networking experience. And I think a lot of our conversation just now really kind of, to me, evokes that. It is like how do I -- a lot of us are giving out information about ourselves. We are posting our whereabouts. We are using devices. We are willingly doing this, so we are all doing it. And that is a kind of a set of issues there.

But let's think about for those of us who work in an organization, we have an HR department. The HR department has a lot of information about us. The HR department is probably outsourcing and contracting with one or two companies. And, in turn, that set of companies is outsourcing to probably another set of companies. And they all have information about you that relates to the provisioning of health benefits, disability, maternity leave, adoption assistance, whatever the set of benefits or HR processes that you get from your organization, chances are, are probably no less than half a dozen to two dozen companies have information necessary for the provisioning of those services. That is happening independent of whether a private or a public cloud is being used.

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

And that balance, I submit, can be struck at some place and level probably but also needs to be kept in mind the type of activity, that the healthcare situation is different from other situations. And we already have a rich history and enacted law in this country that informs the policy decisions that we and the Commission and others would take.

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

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

MS. BERGER: Yes. Please.

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

Right now I think Beth raised some good points about certainly if you have sensitive personal issues, if there is an expectation the information could be used in a harmful way, well, then certainly that is something you would want to know, except most likely if they are going to use it in a harmful way they are a bad actor and they are not going to tell you anyway.

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

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

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

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

MS. BERGER: So okay -- okay.

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

MS. BERGER: So in terms of establishing these positive norms for the delivery of these services, Lindsey, I know you can talk about the negotiation of these contracts, and hopefully some others can talk about, well, what should be them. If that is going to be the mechanism by which we establish these more-protective or more-positive norms, where are we going to get them?

MS. FINCH: Yes. Well, I would just add that each of us are consumers. We all have a place where we live. Most of us have cars, transportation mechanisms. We all have countless relationships with various service providers in our lives. Think of insurance companies, banks you do business with.

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

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

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

MS. BERGER: And before I take the follow-up on that, we have a audience question who -- people may not be quite ready to move on from the idea of informing consumers. And the question is: Is it more important for cloud computing to provide notice about disclosures, who they share with, or what they share or where the data are stored?

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

Yes.

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

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

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

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

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

MS. BERGER: Consumer interest to protect, okay, I think that is an excellent point.

Beth, did you want to amplify the consumer-interest side?

MS. GIVENS: Yes. Just adding one thing, and I guess I am revisiting secondary use, but in a case where there is secondary use -- by the way, my feeling is that if you are dealing with Company X who is then sharing or storing your information with a Company Y, the cloud, first, I think the consumer does need to know that, at least generally.

But when it comes to secondary use I think really it should be a strict opt-in. When you get to secondary usage you get to things that the consumers just have no expectation of at all. And in that situation, yes, a strict opt-in is required.

MS. BERGER: Harriet, did you have a comment you have been waiting to make?

MS. PEARSON: Well, let me actually just sound the same theme a little bit, just to give two concrete examples of the cloud computing uses that might actually just illuminate a little bit more about how to parse out or determine the focus for getting notice or getting information versus areas where it may not be as salient.

So one of the early uses of cloud that we have seen is something called desktop virtualization, which sounds pretty gorpy, but it just has to do with lots and lots of desktop computers. And you get the ability to save lots of money by virtualizing or serving out that computing power instead of having computing power at every desk.

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

Another one is what is known also as server consolidation which goes back to that other era of computing. We had lots and lots of servers. And they're underused and they're turning and they're using up energy. And what people have been finding is that they can save a lot of money and a lot of CO_2 by consolidating the footprint and lessening the CO_2 impact. That's really good, that's great. That does have -- personal information is involved in that because you have lots of different machines that are now being consolidated.

Then the question then becomes: Okay, how do you think about notice then in that context. I submit that's much more of a B2B thought. Then the front business that is involved in transforming its own operations is the one that has the relationship with end-consumers. Then you get back to the same issues we've been wrestling with.

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

Paul, did you want to speak to that?

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

So kind of cutting apart from the consumer, that for me is the big question, and I think what we want to do is move to a sense of reasonable practices are for the cloud and then try to move industry over time, the same way we do in tort for dealing with a whole variety of industrial accidents, so how do we get to reasonable practices so that industry moves there and so that it evolves, so then in ten years -- and I have an answer.

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

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

So again I would say this is the thing: Can we decide, however that happens, what the reasonable practices are that we want to have over time? Then I think it is going to be a mixture of mandatory guidelines from government, negotiated guidelines, whether COPA is a good example or not, maybe some naming and shaming by government of companies that fall short. And then I think a big factor here is adequate liability, because there are all kinds of things in life we should be doing, maybe like being a little more careful in sorting plastic bottles and looking at the bottom, whether it is a 5 or 6 and going back to what the regulations are in our community, which we may not do. But if there is liability, we care about it.

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

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

So let's not forget that a hold at a cloud company is only holding the data on behalf of another company. So of course when we start talking about that first-party company again, we were all nodding and saying, yes, consumers need access to their data held by the company they do business with, and the cloud is just a stand-in for that. So let's not just walk away from the idea that consumers might be interested in access so quickly. The cloud may be an opportunity to deliver on behalf of the enterprise cloud clients to help the company deliver transparency to its consumers, its customers.

Nicki.

MS. OZER: There was an important part of what Anne Toth said, though. It wasn't just access, it was access and control. So consumers could find out what information the company had collected about them. And then there were actually some control mechanisms. They might not be as expensive as they could be, but there are some control mechanisms there.

So I think the importance is about consumer control, not just about consumer access. And so you have to think about that holistically.

You know transparency is good to the extent that the FTC can learn about things that it shines late, that Congress can learn about things, that organizations like us can learn about things and when disclosures have happened. But I agree that there are a lot of limitations to the ability for consumers to absorb this type of information and then to engage in self-protection, because there are limitations to that. That's not really the position that we want consumers to have to be in.

MS. BERGER: I think we have talked about this a little bit already, but does the cloud provide an opportunity? The cloud service and the sophisticated analytical tools that are often present in the cloud, does that provide an opportunity for consumers to learn more about how the companies they do business with are handling and collecting their data?

Lindsey, can you talk to that?

MS. FINCH: So, just to step back for a minute, you know at Salesforce's contracts we say, and this is just in our standard agreement, that we are not going to access customer data, that is, information that our business customers submit into our service except under very limited circumstances. So it would actually be a violation of our contract to provide direct access to a consumer information that one of our customers has stored about them.

But that being said, through our membership with Safe Harbor, if we were to receive a complaint from an individual, we would have to work with the business customer to resolve that dispute.

But I do think that, just to kind of, again, back up to some of the discussions we were having earlier about the massive amount of information that is being kept right now and that is not being deleted because the cost of storage is cheaper than the cost of deletion, organizations and even individuals are being overwhelmed with data. Data clutter, I mean it is overwhelming. And tools are being developed to help us deal with that.

To give a couple examples. So Facebook, I have a couple hundred friends on Facebook, probably a hundred that are very active posters. Facebook provides me mechanisms to sort of filter through the noise. I can look and see these are the status updates I want, so it gives me a means of dealing with that information.

Another example, there is a company called Xobni, it's "inbox" spelled backwards, that helps you to deal with the email clutter that you get so that it can prioritize and help you rationalize the email you get.

I think what the cloud can do in this space is to help to provide tools to help companies better understand their information so that, in turn, they can provide better information back to their consumers. So it's a rather indirect answer to your questions, but I think the cloud computing technology can certainly help their business customers get there to better serve consumers.

MS. BERGER: And so in terms of those analytical tools providing an example for a way to help consumers, you also mentioned the dispute resolution --

MS. FINCH: Yes.

MS. BERGER: -- for the safe harbor. And I think that is a great segue to the topic that Katie is now going to lead us through in terms of data cross-border transfers.

MS. RATTE: Yes. And before we turn back to the international dimension of this computing model, stepping away from calling it a business model, see if Paul and Scott have comments on the last discussion first. We'll start with Scott.

MR. SHIPMAN: Sure. Specific examples, you know we heard on the previous panel that privacy, there was robust competition and that it was a market differentiator for a number of companies. I think that is also true in this space.

When you are looking at -- again, to take a specific example, you can have mom-and-pop businesses processing credit cards, accepting payments, trying to become PCI compliant, and dealing with all of the collection of sensitive information in a very poor or low-tech way, or you can use an online-payment service provider, one that I happen to work with, that does all of that for that mom and pop. And so it does a number of things.

It takes the data out of the hands of a less-sophisticated operator. It enables financial and regulatory compliance, focused on one area of expertise. Now some would argue that it also creates a security vulnerability by having data all in one location rather than a distributed model. But it's an example of where if you were to take that and, say: Yes, and let's add a use policy, let's add retention policies, let's lead as a service provider because it will be a market differentiator for us. Businesses will want to use our company because we make their privacy compliance easy, right?

So it is the same step that Nicole was saying at Google where they are constantly innovating and using privacy as a competition piece directly with the consumer. But in a B2B world it's the exact same story.

MS. RATTE: Paul.

PROFESSOR SCHWARTZ: Yes. I want to make two quick points. To follow up on something that Beth said before that I thought was incredibly valuable was raising the issue of the domestic violence victim. I think something that would be very useful for the FTC is almost if you go to this mixture of mandatory guidelines and negotiated standards and so on and so forth, that you almost red team it, as they do in the intelligence community, where you have a solution and then you have the folks that look at possible vulnerabilities in that solution and to generate lists, like how does it affect the victim of domestic violence, how does this affect this other vulnerable group and are we giving them the tools that they need.

And then on the axis point there was wonderful work on a task force by Deidre Mulligan, I believe, back in the '90s about access. It was a big eye-opener for me because one of the things it pointed out were some of the weaknesses in access. I had always thought up until that point that it is like ice cream, right, the more the better. You cannot have too much ice cream, you cannot have too much access.

But one of the things -- and that might just be my perspective on ice cream, but whatever, if you are more disciplined -- but with access there are real problems that come up with vulnerability to data security. So now I think the FTC has to come in and say if you're providing these access, it is very important that you have these kinds of passwords, you have this kind of encryption.

Then the same thing with controls, which I think allowing people to control information is very important, but all of a sudden you can have someone changing someone's medical record or changing who that record can be shared with. So it is a kind of the department of be careful what you wish for, although I think it is a very important point.

MS. RATTE: Right. I think the authentication point is critical when we are talking about things like access because of the other dangers that you raise.

I want to go back for a second to something that Lindsey brought up which is dispute resolution, particularly when you're talking about in a cross-border context. In fact we got a question from the audience that sort of speaks to this issue. "What legal recourse does a consumer have if their data is compromised in the cloud, particularly if the data are stored in another country?"

So I wonder if some of the business folks on the panel could sort of speak to how you handle this issue and how we ensure that that sort of jurisdictional risk doesn't just land on the consumer. Scott.

MR. SHIPMAN: Well, you know the first question is where is the consumer, right? I mean if the consumer is in the EU and they are dealing with an EU company, well, they absolutely have a right of recourse.

In fact if they are consumers in the EU and they are dealing with a U.S. company and the U.S. company has any location in the EU, they have a right of recourse.

Now is that class action, is that no proof of harm? No, but they have the ability to have the problem remedied, right, and that is through the data protection agencies and the different country-by-country approaches that they have under the directive there that are, at some level or another, harmonized.

From a U.S. perspective, I think the closest level of recourse that we have attained to date would be in probably a few sectoral areas, like security breach. But with security breach the individual has the ability to receive notice and then obviously could pursue recourse with the company that they're doing business. But in fact if you look at the litigation record, there is not a single case yet where someone has successfully sued for identity theft from a security breach. It is rumored that there are a number of settlements that are not public, but there is not a single case out there that I am aware of where they have actually been successful.

And so that either points to either a lack of harm, but that is not entirely the case because we do know, in fact, it does take hours if not months to remedy an actual true identity theft. So there is some harm there, it just has not been successful yet.

MS. RATTE: Do you think there are other consumer-privacy interests, particularly things like access? We were talking about if a consumer is trying to get access to data that may be held in another jurisdiction, are there rules that should be in place here in the U.S. to ensure those types of protections for consumers? I am talking about in addition to the security-breach context that you are talking about.

MR. SHIPMAN: Sure. I mean I can speak, it is a little bit back to the previous panel, it is more in the direct-consumer-to-business model. In a consumer-to-service-provider model I think that is a much tougher question.

As Lindsey said, the primary conduit for access or for any type of rights, grievance, or questions should be with the entity that the consumer or the data subject has a relationship with. But in the business-to-consumer model I think one of the approaches that we are seeing emerge and certainly an approach that eBay has just been approved on is the binding-corporate rules approach that

Europe has adopted.

Take it out of the concept of Europe for a second and just say it is an opportunity that allows a company to say, "these are the standards that we are going to follow, irrespective of largely what law exists." And so for a company like eBay that means that we do provide access. And now certainly we are a new age company, so access is not incredibly difficult. For most companies it is a show-stopper. They simply couldn't provide the level of access that we can provide because our information has been collected digitally. So I mean that is an example, I guess.

MS. RATTE: Yes, that is very helpful.

Lindsey, do you have something to add there?

MS. FINCH: Yes. I think echoing what Scott said about binding-corporate rules, you know with the safe harbor, I know a lot of multinational companies that self-certify to the safe harbor framework do not limit those commitments to European individuals. So I know my company and a lot of other companies that are represented in this room that adhere to the safe harbor make that their global policy. They incorporate that in their privacy statement whether it is with respect to European individuals, U.S. individuals, individuals in India, Japan, you name the country. So that is sort of a not-quite-so-binding-corporate-rule-like way of doing things, but it is an analogous approach where you are taking binding-corporate rules being based mostly on European law, you are taking the same concept with the safe harbor and applying it globally.

MS. RATTE: Right. Harriet, do you have something?

MS. PEARSON: To add to that, just a concrete example to bring it to life, in a business-to-business context let's assume that, again, a large retailer or a large financial-services organization contracts with a cloud services provider or a cloud provider and then part of that data processing may be done in an international location. And if account information is somehow compromised, lost, hacked into, or shared inappropriately, that is I think part of the scenario that we are trying to paint to say what is different about the use of the cloud computing model or the specific equation which is the international kind of processing.

I guess my response to that would be for a couple of decades there has been international provision of data services. These issues have been dealt with. Frankly, there is a recourse against the domestic-based entity that you have the relationship with as the consumer, and then what goes on behind that is kind of not really -- there is recourse directly to that, to the entity.

So I think this is another one of these where the scale of the use and the scale of the international transfers may be causing us -- and appropriately so, by the way -- to revisit and say now let's really think about this because more, more people will be involved in it, not maybe larger organizations that have the wherewithal, but maybe more. So we have got to think through that. And so there are probably mechanisms to do that.

The other thought I would like to throw out may not be right on topic, but I think there is an opportunity within maybe different agencies in government to actually have these kinds of dialogues to try to tease out these practices, these issues, kind of not necessarily -- per necessarily basis but on a basis that says what are these norms and how do you develop them. I think that is an entirely useful exercise, because what we find as well is -- Danny said it earlier, he said -- Danny Weitzner, what did he say -- he said something like growth or innovation depends on the innovative use of information.

I think a lot of organizations are going to be skittish about innovative use of information unless they have some sort of certainty that: Are we doing an okay thing. Am I going to be in trouble. Am I going to be risking something.

Nobody wants to do the wrong thing, not a lot of people want to do the wrong thing, so how do you help them ascertain what those norms -- and I think that is a very valid -- the industry will get there. Business-to-business dialogue will get there, contracts will get there, but I think some facilitation, some dialogue in collaboration with others who have a sense of what's right as well as what is the balance of it I think would be very useful.

MS. RATTE: We think there are probably some people out there who do the wrong thing, but nobody who is represented on this panel.

(Laughter.)

MS. RATTE: We have about four minutes left so I thought I would just throw out kind of a wrap-up question to the panel. And that is: What rules or principles or guideposts for self-regulation do you want to see in the space to vindicate consumer-privacy interests? What's not out there now that you think should be out there?

And I will start with Lindsey and go down the line.

MS. FINCH: Well, I would just say that I know it is off the top of what we are supposed to be talking of in this panel, but with respect to security I think there can be a lot of standardization. I think there are international standards out there that can be followed because a lot of the things we have been talking about, not all of them, but a lot of them can be remedied through good security.

So I would propose things like self-regulation and working towards standards like ISO 27001.

MS. RATTE: Great. Thank you.

Beth. And, Beth, you have already shared with us a number of good substantive things there, so.

MS. GIVENS: Well, just in general I am a believer in the fair information principles, but I have my likes, those that I think are better than others, I think the Canadian set is my favorite, followed by OECD in terms of being robust.

I am heartened to hear that the Federal Trade Commission, I guess, is revisiting the whole issue of privacy principles. And I am glad to hear that because I do think there are some good models out there, but notice, choice, access, and security, that's not enough.

MS. RATTE: Nicki.

MS. OZER: Well, we said a lot in here. (Holds up publication.) I still encourage anyone to get a copy of it if you have not already. And in our FTC comments as well.

But I think just one really important area is the standards for disclosure to third parties. I think that whether it be in the enterprise context or in the more consumer context, it is very important for consumers to be able to trust that their information is safe and that there needs to be higher standards for disclosure. Sensitive information should not be disclosed without judicial oversight. I think that is an area that public interest groups and businesses and government should hopefully all be able to work together on. I know that many people out in this room are already working on that issue. So I hope to see that as well as recordkeeping about how many disclosures are actually made by companies.

MS. RATTE: Thank you.

Harriet.

MS. PEARSON: I guess I would offer a guidepost to be -- you know this concept, it has been referred to before about use. I think understanding there are uses and there are uses, and adopting some kind of a risk-based approach to trying to target the resources of governmental and industry activity on the uses that we think are particularly pernicious, harmful, or just wrong, and trying to address those I think would may be a good frame to try to approach prioritizing.

PROFESSOR SCHWARTZ: I would say there is a continuum here and one end you have command and control, which might not be suitable anymore, where the government just kind of micromanages every algorithm, and then on the other end of the continuum is there is self-regulation of the kind we've seen maybe a decade ago where it means industry is kind of going to do what they want and call it self-regulation. So I think in between that --

(Laughter.)

PROFESSOR SCHWARTZ: -- and in between it is where the action should happen today. And so I think there is going to be room for negotiation of regulations, but I think there is a need ultimately for the FTC and other sectors of the government to have a sense of what should be done, and a normative standard that they then allow industry room around so they can figure out the most efficient, cost-effective, and reasonable way to do that.

MS. RATTE: Scott.

MR. SHIPMAN: Well, I have said it before and actually said it in 2006, we have had guideposts. This is getting more and more complicated. We have got more and more data, moving faster. And I think that while many are opposed to actual federal regulation, I think that it will provide clarity that will help business, not hurt it.

Now of course the devil is always in the details and people become immediately skittish when you say we need actual laws rather than self-regulation. But there are a number of companies out there that have come to that realization and are working on that use-and-accountability model that I think has come a long way since '06, certainly it will take probably equally as long for it to ever happen, if not longer, but...

MS. RATTE: All right. With that note it's time for a 15-minute break. Please join me in thanking this very distinguished panel.

(Applause. Recess taken from 3:02 p.m. to 3:18 p.m.)

PANEL 4: PRIVACY IMPLICATIONS OF MOBILE COMPUTING

MS. HARRINGTON-MCBRIDE: Good afternoon, everyone, and welcome to Panel 4, Privacy Implications of Mobile Computing.

My name is Katie Harrington-McBride. My Comoderator is Naomi Lefkovitz, of the FTC, and we are delighted to be with you here this afternoon to talk about -- maybe I'm feeling sort of proprietary about this now because we have been talking about it so much with our panelists, but I think one of the most interesting issues of the day, which is -- how the mobile devices that we now all carry are transforming not only our lives but also our vision of privacy.

The mobile marketplace has undergone significant changes in the past couple of years, with the introduction of a plethora of new devices that are verging on becoming, if you will, the perfect digital Swiss army knife.

These devices all have great communication benefits. And everything you've come to expect in a cellphone: Voice and texting, email, and -- soon, according to the folks at the Consumer Electronics Show -- even videocalling, which may or may not be advantageous, depending on your view.

Like computers, these devices allow us to store and play music and store photographs and video. We can take pictures. We can play games. We can work on the internet. Magnifying those already-impressive benefits from the device itself are the software applications that further expand the capabilities and usefulness of mobile devices.

These mobile apps, many of which are built in or free to download, can do everything from speed commuters through traffic, help people find their friends or make new ones, enrich visitors' experiences at national and state parks, and even assist a man recently trapped by the Haitian earthquake to give himself first aid.

Mobile devices today use a variety of means to locate themselves, from cell towers to built-in GPS receivers, to wifi-access points.

To ensure that all of these benefits that I've mentioned are available all the time, they can even relay how fast a person is moving and in what direction. It's no wonder that these devices and applications have also raised significant privacy concerns then.

With the potential for mobile devices to provide 24/7 tracking of a user's physical location, along with concerns about retention and reuse of the information, it makes Scott McNeely's famous quote, mentioned carrier this morning, "You have zero privacy... Get over it" sound almost quaint.

In addition, questions have arisen about how effectively the existing privacy frameworks, particularly the notice-and-choice model, map onto the smaller screens of mobile devices.

All of this warrants serious public debate. That is why we are delighted to welcome our terrific set of panelists here today. With us we have, in order:

Michael Altschul, with us today from CTIA-The Wireless Association;

Kevin Bankston, to his left, Senior Staff Attorney at the Electronic Frontier Foundation;

Darren Bowie, Legal Director of North America for Nokia;

Alissa Cooper, Chief Computer Scientist for the Center for Democracy and Technology;

Amina Fazlullah, Counsel for U.S. PIRG;

Brian Knapp, Chief Privacy Officer and General Counsel for Loopt; and

Kristine van Dillen, Director, Industry Initiatives and Partnerships for the Mobile Marketing Association.

So we have a terrific and very-accomplished panel today, experts in their field who can help us to delve into some of the thorny issues in this space. We will use the same groundrules for this discussion as we have for previous ones today, so this will be a moderated discussion.

We will call on you panelists in turn. You should also feel free to contribute to the debate at any time, ideally by holding up your table tent or setting it on end so that we know that you're interested in pitching in. We do have a lot to cover in an hour and 15 minutes, and many, many issues and subissues that we want to drill down into.

We do welcome questions from the audience. I know that there may be some frustration. We've heard a little bit of feedback on the Privacy Roundtable email address. The people are frustrated that not all the questions are being escalated. I can assure you that they are being kept, that the staff will be looking at those and will be considering them seriously. There simply is not enough time in every instance for us, frankly, to even get to all the questions that we have been working on for the last eight weeks. So we will do our very best. Do not be discouraged. Submit them to the privacyroundtable@ftc.gov address.

If you have questions in the audience, somebody will be going around at about the halfway mark and a few minutes before the close of the panel, just wave your card in the air and they will pick it up.

So I think the best place for us to start is to talk a little bit about the complexity of the mobile ecosystem. It's a very fragmented space. And there were some distinctions, some inherent distinctions that we may be need to start by outlining between the mobile and the online space.

So with that, Kristine, let me kick it to you. How is mobile computing fundamentally different than the other online environment we have come to be used to?

MS. van DILLEN: Well, sure, the mobile devices are smaller, obviously. So primarily right there we have smaller screens, so we have got a little bit of an issue with communicating to our consumers all of the things we want to communicate in terms of notice and choice and consent and control, et cetera.

Also the mobile devices are more personal, so we have a situation where the consumers using that mobile device typically are the same consumer over and over again. There aren't families sharing a single device.

Another area is location. So the phone has the ability to identify its location through GPS, wifi, et cetera, any means of that sort.

And then there are other inputs as well that we have in cellphones. So you have got cameras and you have got video cameras and you have got speedometers, accelerometers, and et cetera. So I think when we start looking at all of the different inputs the mobile phone has, you can start considering that not only do you know where you are, you know how fast you are going and which direction you are facing, so that is kind of interesting.

Another thing in the mobile arena is the role of the carriers. And this gets a little bit interesting in that in addition to being kind of the primary function of the customer service provider, they are also the biller. So they are providing the billing function. And, at this point, they are still the primary customer-facing brand. So all of the situations that occur on the phone, even the applications that are being downloaded, the consumers are really looking at the carrier when anything goes wrong; or if any information gets out about them, the carrier is perceived to be responsible on that area.

Then, lastly, and I think this is kind of an important on here, is that the mobile phone has many different channels. And so we start talking about it is not just the mobile internet. We have also got SMS, we have alerts that can interrupt a consumer when they are doing other things. They are not just sitting in front of their mobile phone interacting, they can be interrupted.

So those are the primary differences.

MS. HARRINGTON-MCBRIDE: Okay. Other thoughts?

Darren.

MR. BOWIE: One thought that is useful to make, Katie, is that there are number of different mobile-operating systems. And this is a difference from the online space, where there are not as many. So, for example, Nokia uses a Symbian operating system. There is a Microsoft operating system, Android, Apple, et cetera. While these provide a lot of choices and opportunities for consumers. Technically it can make it challenging to come up with one unified approach to technical solutions to privacy, for example. So that's just a fact that the current different mobile operating systems play a role here as well.

MS. HARRINGTON-MCBRIDE: Another way that that fragmentation issue plays out in this space.

Michael.

MR. ALTSCHUL: Well, when we are talking about the fragmentation, and earlier panels talked about the evolution of computing and the internet, which has certainly evolved but evolved more slowly, the wireless innovation is continuing really at a breathtaking pace.

It seems almost weekly there are new announcements in the paper followed by the product being introduced in stores by the end of that week or certainly next week.

So consumer expectations are driven by the capabilities of all these new devices and network features and applications, which continue to accelerate.

MS. HARRINGTON-MCBRIDE: Are cellphones or mobile devices generally more uniquely identifiable than someone's laptop or desktop computer?

Michael?

MR. ALTSCHUL: I'll take a crack at it.

MS. HARRINGTON-MCBRIDE: Sigh of relief amongst the rest of us. Thank you.

MR. ALTSCHUL: The answers are both yes and no. Every wireless device is going to have a unique identifier or a phone number or an electronic serial number that registers with the network. That is not a personal-identifying information. And, for those of you who are schooled in the Communications Act, a telephone number is not even considered to be part of CPNI under the Communications Act, but it does identify the device.

If you think about your own device or those in your family, the service provider, for the majority of devices, does not know who the user is. It's either a phone that comes from a family plan where the account relationship will be with the mother or the father, then there will be additional phones for children and other members of an extended family. In that case, in the case of four or five devices under one family plan, the carrier is not going to be able to identify the phone number and device with a particular user.

Similarly, those of us who get phones from our employer on an enterprise basis, my carrier has no idea that my particular phone is assigned to me. They know it's assigned to CTIA.

So the code is a bit broken even though the device has a unique identifier.

MS. HARRINGTON-MCBRIDE: Alissa.

MS. COOPER: We have already had the two somewhat contrasting notions about how identifiable the device might be because, as Kristine pointed out, that mobile devices even when they are not attached to a name are quite personal. I think if we think about the service that Peter Eckersley mentioned this morning that EFF launched yesterday, the Panoptoclick, where you can use your browser and go and through the service find out how identifiable your browser is, I would be surprised if the same sort of logic doesn't apply to your phone. And that by using your phone or your mobile device just for a short amount of time, the pattern of behavior and the data that gets resultingly stored on the device because you're the only one using it becomes actually highly unique to you. It just seems logical that if you are the one who is always using the phone, then that fingerprint of the phone really starts to become something that is unique and can identify you.

MS. HARRINGTON-MCBRIDE: I think that is a great beginning. I wanted to just sort of set the stage, just sort of set some of the distinguishing factors out.

And, with that, I think what we would like to do for the balance of the panel is to work from a hypothetical and Naomi will begin with that. And then we will ask you all some questions about that and try to get at some of the thornier issues relating to location and device size.

MS. LEFKOVITZ: Right. So we did not think we could really come to a law school and not come out with a hypo, so it would be particularly disappointing to the law students in the audience.

So today we have a little bit of a story about Agnus. Agnus is driving to a job interview. She is on the verge of being late. She uses her mobile to check on the traffic and sees that the way she was planning to go has traffic delays. So she takes another route and makes it to the interview on time.

It is mid morning by the time the interview is done. And just as she is thinking that she deserves a latte, the coupon service she signed up for sends Agnus a coupon for a nearby coffee shop.

After her coffee she wanders around the downtown area window-shopping. She comes across an interesting street performer and she uses her mobile to snap picture, which is automatically geotagged showing the latitude and longitude where it was taken, and uploads it to her social-networking page for her friends to see.

It so happens, though, that in the background of her picture is a man and a woman kissing. And, as it turns out, this man happens to be the husband of a friend of a friend, whom that friend believed was on a business trip. So, in fact, all is revealed when the wife browsing a social-networking site later that day notices the photo while visiting her friend's page.

But back to Agnus. It is now close to lunch time. And last night Agnus had made some big plans to meet up with friends. So she checks her friend-locator service to see who's around. She also opts to broadcast her hunger and her location to her Twitter account.

Giggling slightly, she reads a ping from someone who has a profile on her dating service that noticed she was nearby. But then the service also sends her an ad for a nearby bar. And, ugh, she thinks, I may be jobless but I'm not so desperate that I need a drink in the afternoon. So she hits the opt-out for advertising and clicks out of the service.

So now we are going to ask some questions of the panelists. You can use the hypo as you see fit or other issues that you think, but we think we have provided some interesting issues here.

So let me start with Kevin. So a couple years ago, right, the main actors in the mobile ecosphere were handset manufacturers and carriers pretty much, but today, as we have been already starting to hear, we have operating-system developers and a potentially-infinite array of application developers and behind them sits the whole online apparatus of advertisers, analytic companies, so on.

So what laws apply to how consumer information in the mobile environment -- how is that consumer information treated and where do these laws fall short? What, if anything, is filling in those gaps?

MR. BANKSTON: Well, first off I would like to say I consider myself fairly expert in this area, but if I were to get that hypo on a privacy-law exam I would run crying out of the room.

(Laughter.)

MR. ALTSCHUL: So we got it before the exam.

MR. BANKSTON: Indeed.

MR. ALTSCHUL: Unlike in law school.

MR. BANKSTON: But basically my message here is that the existing statutory rules that apply to location information are incredibly decrepit and woefully inadequate when it comes to this new dense, complex ecology of service providers, handset providers, OS providers, first-, second-, third-, fourth-, sometimes fifth-party application providers.

I was looking at this chart, which you might want to look at too, and thinking about all the things that were not on there, first and most notably, the carrier, the OS vendor, the handset vendor -- I'm looking at you, Palm Pre, because it was recently reported that their handset secretly sends your GPS location to Palm every day for some unknown reason -- then the providers who are the backend for the providers here, like the backend of the advertising service and whatnot. And so you have this broad ecology of companies and services that have access to this data and two really old statutes governing or, in most cases, not governing what they can do with it. One of them is 24 years old, one of them is 14 years old.

The 14-year-old one is 47 USC 222 from the Telecom Act of '96. And this classifies wireless-location information about your cellphone use as customer proprietary network information, CPNI. And so there is actually a bar on your telecom carrier disclosing that information without your consent except in emergency circumstances.

But a few caveats: It does not apply to aggregate information from which identifying features have been removed. And, most importantly for our purposes today, it only restricts telecommunications carriers. It does not restrict any of these other entities that we are talking about.

For broader restrictions you need to look to a law that was written when the primary focus of networking and computing was dialing into your BBS, and that's the Electronic Communications Privacy Act of 1986, which has been amended a few times in a few ways in a few ways, but primarily has the same structure it had 24 years ago. And that law restricts voluntary disclosures by a couple of different types of entities: Remote-computing services and electronic-communication service providers.

I will not belabor the point by reading the definitions, but suffice to say it is pretty clear your ISP and your phone company are electronic-communication service providers. Moving beyond that, it is actually quite unclear what entities are covered by this law, and which is an ECS and which is an RCS, because there are differing rules for both and so it matters.

But this law not only regulates voluntary disclosures by the companies but also when the government can mandate disclosures from these companies, which is obviously our focus as civil libertarians as you might note from the "Come back with a warrant" sticker on my computer, but focusing on voluntary disclosures, whether or not a company needs your consent to disclose something depends on whether the information is communications content or noncontent information about your use of the communication service.

So in the typical scenario, that is the location information that your phone company has, reflecting your use of their phone or internet service, that is noncontent information and the company can disclose it without your consent. I think there are a few cases where your location information is indeed content, such as friend-finding services like Loopt where you are sending your location to other users of the service. And we are glad that Loopt and Google's Latitude have taken that position, which we agree with. But in many if not most cases the location information is going to be considered noncontent at least by the carrier or the service provider such that it could be disclosed without even your knowledge or consent.

And so the current statutory regimes are really quite underprepared in dealing with this proliferation of services that have your data. You know not only is it weakly protecting the data even to the extent the law applies at all, in many cases the law won't apply at all because the service doesn't qualify as an electronic-communication service provider or a remote-computing service.

So if you are looking to the federal statutes to help you, it is not looking very good.

MS. LEFKOVITZ: Darren, do you want to speak?

MR. BOWIE: So in addition to the statutes that Kevin mentioned, I would point out a statute that now is nearly a hundred years old, and that's the Federal Trade Commission Act. And we should certainly point out that that statute has a very important role to play in this hypothetical, in addition to all of the state deceptive-practices statutes modeled on the FTC Act.

So a number of the parties in this hypothetical are subject to FTC jurisdiction. So all of the third-party application providers here, the dating service, the coffee-shop coupon service, all of those are subject to the FTC Act. And they have a duty, of course, to disclose all the material terms and conditions of their service, including are they receiving and using GPS information, how are they using that information, are they going to be sharing that with advertising networks, with advertisers. And I think about this issue about the ad for the bar that the person received.

So it is important to realize the important role and the flexibility of the FTC Act when we look at this hypothetical, in addition to the statutes that Kevin mentioned.

MS. LEFKOVITZ: Alissa.

MS. COOPER: Just to go back for one second to the CPNI rules, we have talked a bit today about the Fair Information Practices. I just wanted to reenforce the point that not only do the CPNI rules only apply to the carriers, but whether you think the FIPs are broken or you think we have not done enough to address all of the FIPs, the CPNI rules don't come close to addressing the full set of Fair Information Practices. They are really only about disclosure and sort of nominally about consent. So there is nothing in there about security or access or minimization or any of the other Fair Information Practices.

MR. BANKSTON: I will add a clarifying note building on that. The ECPA -- Stored Communications Act portion of the ECPA and the CPNI rules do not restrict use or retention in any way. It is all about disclosure, so.

MS. COOPER: One other note on the hypothetical. I think we tend to think with the proliferation of smartphones and all the app stores that are out there, we think a lot about these cool new apps that everyone has on their mobile phones and, in particular, location-based apps. I just wanted to draw people's attention to the fact that it is not only apps developed for specific platforms that can gain access to the mobile device and to things like location information, but it is also Websites.

Last summer there was actually a draft standard put forward that would standardize the way that Websites can ask Web browsers for your location information. And all of the major mobile browser platforms have implemented it.

And what this means is that, as opposed to the scenario that we have been used to and that Darren mentioned at the top about having to develop applications differently for each kind of platform, what the Web did for desktop computing it also has the potential to do for mobile computing. And what that means is that we have the potential to see many, many, many more Websites that can gain access to the mobile, gain access to location information much more easily because they can be developed just one time for the Web.

So some of those apps that Agnus may have used in the hypothetical, they do not necessarily need to be purpose-built for one device. They could be built one time for the Web and used on any device.

MR. BOWIE: One other thought too, we are talking about the laws that apply, but of course there are significant self-regulatory initiatives that apply as well. So, for example, and Mike can certainly speak to this, CTIA has issued location-based services guidelines. To the extent the actors and providers in this hypothetical are members of CTIA, they are bound by those guidelines. Also the MMA has guidelines that would apply as well.

So I think it is important to consider those guidelines. We can talk about how effective they are, but they are relevant to the situation.

MR. ALTSCHUL: That is actually why I had raised my tent. I think there has been for some time a recognition that the statutes do not reach where the technology and the applications are today. And a little history might be helpful.

The CPNI rules were passed as part of the '96 Telecom Act, but there was no reference to location as proprietary information until 1999 when an amendment sponsored by Congressman Markey was passed. And that was because the FCC in about this timeframe had mandated that wireless carriers provide location information in connection with 911 calls.

As a result of wireless networks gaining the capability to actually identify a user's location on a much more granular basis than was possible before, Congress amended the statute with carriers and the kind of technology that was being contemplated more than ten years ago in mind.

As we already discussed on this panel, increasingly the carrier is not going to be involved with either determining the user's location or even in transmitting it to the application. Most of us or many of us who now have smartphones, I started to say "many," it is not going to be long before it is a majority of users, wifi is built in to the devices as an alternate transmission path. Depending on the operating system, the phone will default to the wifi network before the wireless carrier's network, at which point the user will never know which air interface is being used, but the location information and instructions to the application will be sent without ever touching the carrier's network.

Two years ago when CTIA started its best practices for location-based services, based on the Fair Information Practices of the Federal Trade Commission, we had assumed that carriers would be central to the determination and transmission of the user's location. We have just gone back and are in the process of revising the scope of our guidelines and best practices to recognize the fact that in two years the world has changed and increasingly devices and applications are not just agnostic to the network but oftentimes independent of them.

MS. LEFKOVITZ: A quick last word.

MS. van DILLEN: Yes. Darren also mentioned the Mobile Marketing Association Global Code of Conduct and I just wanted to highlight the pieces of that which include the notice and the choice and consent, customization and constraint, security and then enforcement and accountability. And those are the expectations that the Mobile Marketing Association has for mobile marketers.

MS. HARRINGTON-MCBRIDE: So obviously this is a very complex ecosystem, to use an overused word yet again. And there are a lot of factors at play. I think one of the things that we really wanted to hone in here on is elucidate for us some of the underlying concerns about access to locational data. Because, obviously I'm with Kevin, I would be at the water cooler doing my Yoga breathing if this were my exam time. It's a very complicated hypothetical, there are a lot of people in play, there would be a lot of analysis that needs to be done, and obviously we only have 40 minutes or so remaining, so let's talk about at a high level. What are some of the location-privacy concerns and then how do they play out differently depending on who is obtaining that location information and how responsible those parties are?

So who would like to tackle that one?

Amina.

MS. FAZLULLAH: I am going to talk about some of the harms, but I guess briefly I think when you realize that people know your location, I think there are a few things that can start to come up. If an employer, so if an employer is resource tracking, like using a mobile phone to know where their bus drivers are, where their crossing guards are, where other employees are, if they don't give the employee the ability to have some kind of privacy control, then they now have information on what the employee is doing even on break, perhaps even after hours. So there can be employment issues related to that, employee-privacy issues related to that.

I think that especially with healthcare there is also some issues. If information about kind of where you are spending a lot of your time, if you are going to -- it can be identified that you are spending a lot of time in a hospital, a doctor's office, or some other location that can give people an idea of what your healthcare situation is like, that can have some kind of effect down the road in terms of access to insurance, or just depending on how that information is distributed, how granular it is, what is said about it, who else is having it, that all can affect your opportunities for services down the road. I mean that is just picking one particular piece of information.

Then there is also sort of identifying people that maybe you don't want to know anymore. So worrying about domestic violence issues and whether or not somebody will now have access to your location, say, through social networking, through friends of friends. Kind of going back to the hypothetical, there are some issues related to that where you can clearly see if people actually know where you are and somebody down the road, because your information is kind of getting distributed pretty far, can actually come back to haunt you, somebody else that you do not want to interact with you can come back.

I think that is just sort of the obvious ones, but then there is also just consumers interacting through their mobile device, purchasing, using, sort of the transactional capability, having financial information. Those are things that we also start to worry about.

Exactly how secure is it. Now that you are putting all of this pressure, say, on your carrier as some place to transact through, you know what does that mean, what kind of responsibilities are you giving to the carrier. Is that something you had expected.

Then there are also issues related to sort of political speech in a locational device in location so that if you are identified being in a particular area during a protest, what does that have to do with civil liberties. If you are getting texts when you are at a polling location, beyond the point where you are supposed to be getting any kind of information related to a candidate, that also has some implications.

So it can go pretty far. I think people can sort of understand how it can sort of getting to used in multiple ways.

MS. HARRINGTON-MCBRIDE: Brian.

MR. KNAPP: Yes. I am glad Amina walked me through some particular situations because I do think you need to think about it a little bit specifically. I mean for a minute there I freaked out because I realized everybody here knows where I am and they know my location. Kevin's here and I knew he would protect me, but I think there are a few situations where it matters, right.

So domestic violence and safety I think is something -- it is sort of another path, and we have done a lot of work in that area. I think it is a little outside the scope of this discussion, but I think with regard to employers having access, government having access over long periods of location-history information, I think that is a sensitive situation. We are involved in the ECPA reform that both CTD and the EFF are participating in and pushing really hard.

We are concerned about passing complex -- you know this is a complex situation, so to pass more complex, outdated laws to replace current, complex, outdated laws concerns us. Definitely what Darren said in terms of the FTC's enforcement authority is something to keep in mind here, and we do think it applies.

We believe the industry is doing a great job in terms of self-enforcement and we think there are a lot of responsible parties in the mix, such as Loopt, such as Google, such as Facebook, and Twitter.

And the one thing I did want to point out is that the innovation with applications that have been unlocked by location information, these mobile devices and now the iPad, are second to none. And users are thriving on these services, right. So they are using navigation, they are using local search to find out what is happening around them whether it is their friends or events or restaurants, and they are really consuming these applications I think in ways that we never before imagined two years ago. And that is a really positive thing and I want to kind of keep that in mind here, because you are not only driving innovation but you are driving revenue opportunities, you are driving employment, you are driving an entire technology industry that is based on the opportunities that these applications have to provide services and sometimes, yes, contextual and relevant advertising in a certain moment in time.

MS. HARRINGTON-MCBRIDE: Yes. And I think Brian raises a great point which goes to the question of maybe retention of this data. So clearly, Brian, because you are here and we are going out on the Webcast live, everybody knows, your secret is out, you are here at the FTC's Privacy Roundtable Number 2. And --

MR. KNAPP: You are keeping it for...?

MS. HARRINGTON-MCBRIDE: About a year is our typical retention period.

MR. KNAPP: Okay. Is that on your Website?

MS. HARRINGTON-MCBRIDE: I got to tell you, we are doing this through Berkeley, so you have to check their terms of service.

MR. KNAPP: Okay.

MS. HARRINGTON-MCBRIDE: But I wonder if you would feel differently --

(Laughter.)

MR. KNAPP: So you guys are a third party in this? Oh, this is -- is that okay?

MS. HARRINGTON-MCBRIDE: So your point is well taken, that you are here and everybody knows you are here, but would you feel differently if Kevin were to follow you around for a year and then publicize your whereabouts? So how about retention of data? That is something your company has dealt with in a particular way. Can you tell us how you have done that?

MR. KNAPP: Sure. So we tend to look to the user, right, so we try to get out of a legalistic sort of framework and mindset with this stuff and say, okay, what do we need to drive our business and what does the user want us to do, sort of, on their behalf. And we think those are the important areas to look at it.

So we do think location is the kind of thing that is less sensitive on a one-off basis and more sensitive over time. So we had to provide our basic friend-finding service need to have a location fixed at a given period of time, right, to show where you are, based on your settings and what you have opted into, et cetera.

But otherwise to provide that basic friend-finding service need, we do not need to keep that location any longer. And we also don't need to keep it to provide you relevant content or relevant advertisements around you at a moment in time. So we use that location fix and we don't maintain it any further unless you do something with it.

So in the example where our friend Agnus tags a picture and posts it up and she might use Loopt to post that out to Facebook or Twitter or the Web. And as long as she keeps that up there, as long as she keeps that in her Loopt account or Loopt journal, we'll maintain it on her behalf, she deletes it, it comes out of our systems. So we're basically using it and we don't really have a use for it, we don't have a business use for it to maintain that location unless Agnus wants us to keep it on her behalf or to otherwise provide the realtime location tracking and friend finding and relevant information around you that we already do for our service.

And it is interesting because there is a bit of a tension, and we talked a little bit about safety. In Amina's examples there is a tension between law enforcement and what sometimes the government asks you to do with regard to retention and what the privacy side of it is. And so we also -- and again thank you to the EFF and CDT has sort of helped us figure out some strong policies around that with regard to not only our retention but what the legal requirement is for access to that information.

And we have taken a position I think that reflects where we all want to see ECPA go. We have taken that position sort of before those changes come in place.

MS. HARRINGTON-MCBRIDE: Kevin, since we keep invoking your name I am actually going to call on you for once.

MR. BANKSTON: Sure. I mean to expand and reiterate on some comments and maybe belabor the obvious, this is a rich vein of new data that simply has never existed before. And although technically when you were in public that was public, unless you ran into someone you know or, God forbid, someone was trailing you, it was practically obscure. And the citizenry could be free to go to an Alcoholics' Anonymous meeting, go to the family-planning clinic, go to that cancer specialist, attend that secret union meeting, attend that controversial political or religious gathering with some freedom and anonymity.

Now there are records that can reveal those things. And, to a great extent, the collection of that information and the handling of that information is unknown to the person carrying the phone or other mobile device.

And I also think it is important to note that just as we were talking about in the social-networks panel, there are front-end and back-end issues. There are the back-end issues of who is collecting what and how long are they keeping it and what are they using it for, but there are also the front-end issues of how are you managing the sharing of that information with your friends and are you inadvertently disclosing more about your location to your friends than you actually intend. Are you going to accidentally allow your employer to find out that you went to that secret union meeting or your wife to find out that you went to that iffy bookstore.

And so there are several levels here and it is not similar to the social-networking issue.

MS. HARRINGTON-MCBRIDE: Alissa.

MS. COOPER: One other property of location information which I think makes it special that has not been mentioned yet, and I usually use myself for this example but I will use Brian since he is the privacy fundamentalist on the panel.

There is only one person who spends his daytime hours at Loopt and his nighttime hours at Brian's house, assuming that your wife does not work at Loopt and your dog does not have a cellphone, and that is Brian.

(Laughter.)

MS. COOPER: And that is Brian, he is the only person. And so it does not take very many days of collecting that location information from Brian's device to figure out that it is him, not knowing anything else really other than having a phone book, basically.

I think that -- it's something that is special about location. It is the reason why some companies that collect location information have done things, like cut off the two ends of every trip that they collect so that if you are using navigation directions, Google, for example, does this with their traffic data, they will snip off the ends of each trip because -- and kind of randomize it -- because those two ends can be used to identify you. It is another reason why retention is so important, because if you retain that pattern over just a small number of days, you can start to identify someone.

So it is not the case that it needs to be married to an identity. In and of itself, the behavioral movements tied with location can identify a person.

MR. KNAPP: I am going to jump right in. So I think that's right, but I think just to use those two examples, gazillions of people know where I work and a lot of people know where I live to, especially a lot of direct-marketers have my location, have my home address. All my neighbors, a number of folks who have been over for dinner parties. And so those two locations are not a secret for me at least and I have not made an effort to keep them private from folks.

So to the extent that Alissa is talking about using those locations to then identify me as a person, reverse-engineer and use some other -- tie that to other information and things I am doing on my mobile device, I guess that is a path we could go down. But I want to point out that location in that example is really only a means to identify that it is me with a phone and there are probably other easier ways to do that. In fact, I have probably given a lot of these mobile applications my name and information and email address. My wireless carrier has my information, perhaps tied to my phone number.

So I just want to point out that those

particular locations and, yes, I am usually at home at night and I am usually at Loopt during the day, are just not a big secret, right? And that is my point around being really specific about when location becomes sensitive and in what context and vis-a-vis what kind of parties.

MR. ALTSCHUL: To follow up around the dialogue between Brian and Alissa, certainly some, probably the overwhelming majority of location information is not going to be troubling to the user, but there will always be a category of information which the user would not want shared. And that gets us back to the notice and consent and the control principles that are central to all of the privacy discussions.

And going back to our now-forgotten law school hypothetical, each of the different applications indicates how the user has had to opt in to a particular application, whether it is realtime traffic and GPS navigation or uploading to a social network and posting on Twitter a photograph, a lot of settings have to be enabled by the user, not just the click through for the scrolling of the consents but the phones need to be provisions, software needs to be downloaded, there are choices as to how the information is to be displayed, what kind of information you get back. And it is sort of common-sensical that the more the user has to interact with the application, the better understanding and better control the user is going to have of that information.

Just as an aside, my favorite part of the hypothetical, of course I think we all recognize, was the photography on the street being uploaded. This is a plot from an opera, actually. It would be a very, very good plot for maybe the first new opera of the twenty-first century.

MS. LEFKOVITZ: Well, that is a really good segue on the issue of notice, so we are all very interested in what kind of experimentation is going on in this space with respect to notice. Is there any research or feedback on how consumers are viewing this?

Brian, do you want to...

MR. KNAPP: I think the top Web and mobile companies out there are some of the best around in terms of handling this stuff. So I think Apple, for example, the location-based applications, it is hardcoded into the OS to provide a quick, translucent notice to let them know that an application has accessed the location API in the iPhone.

So it is informative, but it also does not create a lot of friction between the user and the application that the user does not want. I think other

OEMs and manufacturers are doing that as well, so I think Google and Android are doing a nice job in that regard and Rim with BlackBerries as well.

I do think the mobile environment need to be particularly in tuned to the size of your notices, if you want to come across to the user and have them understand sort of what they are participating in. And, again, I think that is why it is best to look at it from sort of a customer-service and product-development and a privacy-by-design perspective versus sort of trying to check some legal box.

We do not believe opt in is some sort of magical silver bullet and we get concerned when people throw it around that way, but we do believe that users should have a sense of what an application is going to do when they open it and to the extent notice is appropriate.

I do think that there is an expectation and there is going to be an expectation by users that these smartphones can locate themselves. Often it is put, especially sometimes in surveys and such, where they will ask, 'Well, you know if such-and-such was tracking you all the time, how would you feel about it,' well, I bet if you asked it a different way and said to the user, 'Do you expect your $400 smartphone to be able to locate itself,' I bet you would get a similarly high response.

So I think users have an expectation that these mobile devices can locate themselves and provide them with robust services on top of that location infrastructure.

MS. LEFKOVITZ: Well, I guess that brings us sort of an interesting point, because there is this sort of linguistic discussion going on here between locating, right, the phone happily locates itself versus tracking, which I guess has a more nefarious sound, right?

So I guess that is sort of the tension that seems to be going on here today; does that sound right? Does anybody want to... Amina.

MS. FAZLULLAH: I would say that makes sense. I think that maybe where it would be helpful is to look at the use, right. So when a consumer is asked the question that you just posed, 'Do you think your smartphone can find itself,' and think your expectations of what that means or how it is being used would be different from, say, the nefarious tracking. And then what that would actually be doing.

So I think when you give -- so to go back a little bit, if you were to give consumers control over how commercial applications are used versus, say, whether or not you want your phone to be able to dial into an

E911 service without them having to do anything like special, I think people would sort of break down in two different packs.

I think if you wanted to have maybe some security measures so if your phone is stolen that you can identify it or if you are doing some kind of product location, if you have like a car that's stolen, you want to identify it, this is a little off the map, but again people would take that differently.

So I think it breaks down to use: How is it being used and who is using it. And so that is when locational information actually -- that is when notice and consent start to really come in because they are just expectations from your service provider, what you expect them to be able to do and why they would need to know that information. And then there are expectations from the other commercial applications that you are using and why they would need that information and who they are sharing it with and what it is being used for.

MS. COOPER: I think notice in the form of the screen that pops up to ask you if it is okay to share your location in this instance is one aspect of transparency and involving the user in the decisionmaking, but it is really only one small aspect.

And I agree with what Brian said, that many of the platform providers have done a good job with the upfront consent. So when you go to a location-enabled Website, when you use a location-based application it will ask you if this is really what you want. But it does not stop there and many of the platforms seem to think that it does.

So if you want to see a list of all the applications that you have given your location to, if you want to be able to create a white list or a black list so that you don't have to go through the opt-in process every time or so that some sites or some applications can just never have access to your location, if you want to get a reminder every now and again of which sites or which services you have given your location to, I know that is a feature that Loopt includes but it is not a feature that every platform and every application includes, and I think that more robust notion of transparency and of involving the user in the choices that he or she may have made a long time ago, is really the more robust kind of notion that we should be focusing on as opposed to just like when the screen pops up what do you click, did you understand.

MR. BOWIE: I would agree that the concept of use is very important here and I think, again, it comes up in the hypothetical. If you read the hypothetical you can assume that there are some situations where our consumer seems to be surprised and not have expected when her information has been shared.

I think, again, we have to come back to what does a reasonable consumer expect about how their information is going to be used. I think they do expect that information will be shared with their carrier for certain technical-related reasons, but here she did not seem to expect that she would be getting an ad from a bar. So I think it is useful to look at what disclosure was made to her and how that should have been made.

So privacy settings are very important and I absolutely agree there is a lot of work to be done in this area to bake privacy settings into the device and through platforms. But, as we do that, we have to focus on where is the harm to the consumer and what are their expectations, and this hypo is an example of that.

MR. BANKSTON: Yes. My iPhone is saying Google Maps wants my location. That is one type of notice, but it is not notice at all in terms of how long Google stores that data, whether and what steps it takes to deidentify it, et cetera, et cetera. Something that Google has not made public.

And you know we had people like Facebook and Google coming up and saying, we are the good guys and we are here to talk to you about what we do and be upfront. And even they, we do not really know exactly what they do.

You bring it closer to home and people do not even know what records their carriers are storing. Again I like to think I am an expert in this area, I have seen a handful of exemplars of what types of cell site records companies keep, but I do not know what the standard practice is, how long they keep it, whether they deidentify it.

So I think there is a real serious problem in terms of consumer knowledge or regulator knowledge about exactly what is being collected by whom and what they are doing with it. We do not have all the answers we really need to those questions. In fact, not only is about notice about use or disclosure or use, also disclosure about capabilities.

For example, even if you do not use any GPS-based location-based services your carrier can still obtain your GPS location, as was most recently established when Sprint announced at a surveillance conference, described the interface they have set up for law enforcement to go and obtain your GPS location without your knowledge.

So I do not believe notice and consent is a silver bullet. I also think, though, however, that notice is incredibly important and people are not getting notified enough of what is going on.

MS. HARRINGTON-MCBRIDE: Notice -- oh, Amina.

MS. FAZLULLAH: I just wanted to add one more point, is that with notice comes control. So I think what is maybe a positive benefit to marketers or applications providers, when you send them an ad for a bar that they do not want, if they are able to say, hey, you got it wrong and here is what is right, because they actually want to get the right stuff, you provide a platform where the consumer can now trust you and have a relationship with you and correct things when you get it wrong because they actually want to get stuff that's right. I think that would be really hopeful for the industry and it would grow control for consumers and they would actually be able to understand, actually participate in the process of giving their information and getting something back for it.

MS. HARRINGTON-MCBRIDE: Okay. Kristine, -- I would love to have --

MR. ALTSCHUL: If I could follow up, since Sprint is not here to defend their honor, I think we have all agreed that the scope of what access law enforcement has or civil subpoenas have to this information is beyond our scope, but in the example Kevin gave it actually was an example of law enforcement pursuant to a warrant --

MR. BANKSTON: I didn't say it was pursuant to a warrant.

MR. ALTSCHUL: Well, law enforcement gained the -- every time you receive a warrant --

MR. BANKSTON: For legal process.

MR. ALTSCHUL: For legal process. Every time you receive one, just as -- let me -- have it on the back of it -- the service provider is prohibited from providing notice --

MR. BANKSTON: Well, that --

MR. ALTSCHUL: -- so that I just want to -- I know you did not intend to be misleading, but for those in the audience who are not familiar with the particular context of Sprint's statement at a conference on this, they should know that in that particular example Sprint, pursuant to the process they received from the government, could not give notice to the customer.

MR. BANKSTON: To clarify what I was criticizing, I was criticizing the fact that consumers do not understand that their GPS can be remotely turned on and accessed by the carrier, not that the government can use legal process to secretly do so. It was a fact about people not understanding the technical capabilities that exist, so.

MS. HARRINGTON-MCBRIDE: Okay. So, Kristine, I would like to talk to you a little bit about advertising in the mobile space. Obviously location by some accounts from marketers is the holy grail. It is the thing that everybody wants. Because if you know where people are, you have some context, you have their information about what they are close to, and you can probably very readily monetize an advertising structure.

So I want to get to that because we only have about 15 minutes left, so tell us a little bit about your perspective on the things that we have talked about about notice that may impact advertising. So, for example, a consumer may opt in to a service and know full well that they are using it for their own purposes to, for example, find out where their friends are in a given space or to get directions to something.

To what extent are consumers aware that advertising is part of that business model and then to what extent do they have control, as Amina suggested, over what advertising they see?

MS. van DILLEN: Right. Well, we see that location-based advertised is many more times valuable than regular advertising, so that is many multipliers. And our recommendation is is that you give customers consideration for when they provide you with information as an advertiser, which means that if a customer is providing their location to get information about what is around their location, they would reasonably expect that that location is then being shared to provide advertising back.

We find that consumers are familiar with that behavior online, they expect that advertising is going to supplement the data that they are receiving for free, and so I think it is very important to note that it is that consideration, it is: I am a consumer, I'm supplying you with my personal information because in turn you are giving me information that I am looking for for free.

MS. HARRINGTON-McBRIDE: Sounds like it may be akin to the online model.

Ms. van DILLEN: Yes, and we find that the consumers are comfortable with that, that that's what they expect.

MS. HARRINGTON-McBRIDE: And so does that expectation -- to what extent do you think then, for example, consumers would understand behavioral advertising in the mobile context? And to what extent is behavioral advertising combining, for example, that locational piece into a broader profile of a consumer and their interests and habits, how is that data being married up?

Ms. van DILLEN: Right, and so I think that is bringing up the more complex point, is, okay, once you get beyond that one-for-one trade-off then you bring in the behavioral advertising and then we go into the self-regulatory principles of behavioral advertising that some of the other associations have put out there. And those are the ones that we recommend marketers and advertisers follow at this point.

MS. LEFKOVITZ: So in the hypo Agnus was able to opt out of the bar ad because she did not like it and it was offensive. I mean is that possible?

Ms. van DILLEN: Absolutely. So it depends on what type of service she was using. But in certain applications you are able to choose which brands or which companies you want to be interacting with, which bars you want to be interacting with. SMS functionality, you would be able to opt out of that. There are actually WAP ads at this point, some ads on the mobile browsers, that you are able to opt out of certain brands. And we find that advertisers are very accepting of that because then they can deliver ads to the people that are accepting of their brands and that want to engage with their brand.

MS. LEFKOVITZ: So how do they know how to do that? We really heard, again, how complex this world is, I mean how does a user know how to manage their privacy? Do they have to go into their device settings, their OS settings, their carrier-privacy policies, their application?

Ms. van DILLEN: I do not think it is that complex right now. I think in a lot of cases it is setting up an application and it is selecting the different types of brands you want to be engaging with. I think because that provides a value for the consumer and for the brand, that that's one of the first setting features the consumer comes across when they select that application. The way I have seen it set up on the banner ads, it is a menu icon on the side and it is something that the consumer clicks for more information, and there are a list of things and they can opt out in that way.

And then for text messaging there is always an option to stop text messaging. And we are very clear about the guidelines for doing that, making sure the consumer understands that they can always press stop to stop text messaging alerts.

MS. HARRINGTON-McBRIDE: What role does government regulation have to play in this space going forward? We have got about ten minutes left, so let's think about the self-regulatory standards to some extent are in place. I know Mobile Marketing Association is still looking at finalizing location-based service regulations.

Michael has told us that CTIA is revising and trying to take account of some of the rapid changes that have taken place.

So what are the standards that should be set, whether they are set by a government agency, a self-regulatory body, what should be the baseline code of conduct for behaving responsibly in this area?

MR. BOWIE: So I can start with that, and there are some important self-regulatory initiatives already in place, and we have discussed those. I think there needs to be further work done on refining some of those initiatives to the unique issues involved in the mobile ecosystem.

So there has been a lot of discussion about behavioral advertising. Are there specific aspects of mobile behavioral advertising that need to be addressed, certain different types of disclosures or other ways to do that. So that is work that should continue.

When we get into the question of government regulation in this area, I think before we get to that there are two things that the Commission, to take an example, could do now before we consider whether additional regulation is necessary.

One, I think there is a very important role in consumer and business education, and the Commission has done an outstanding job in other areas. In the last decade, the Commission produced a very important education piece called Dot Com Disclosures, on how to make disclosures in the online environment. I still have my very old dog-eared copy that I actually still use.

I think something targeted to mobile disclosures and with examples and when a just-in-time notice might be appropriate, I think that would be very important and something the Commission could do now while we think about these big questions about regulations.

Also I think there is a role for increased enforcement in this area, so the Commission has done an outstanding job in privacy enforcement, I think some enforcement targeted in the mobile space also would be useful to send a message that this is an important area that's a priority. I think it is fair to assume that there are bad actors involved here who are using information without proper disclosure and consent, in nefarious ways. So some increased enforcement by the Commission also would be important.

And the state should also be engaged. I wanted to make that point as well, the state AGs should be involved in these discussions. They are going to become involved in enforcement, so it is important to include them as well.

When we move to the question of regulation, I do think this is an area, because there is so much innovation, there is so much change, as Mike pointed out, the mobile world really has changed almost completely within the past couple of years, to me it would be difficult at this stage to come up with regulations, given all the changes, and the opportunities I just identified to take action in this area already under Section 5 and existing law.

MS. COOPER: So I am really glad that Darren brought up enforcement because otherwise our panel would have been the only one to not suggest that our friends at the FTC engage in more enforcement, and I think he is absolutely right that this is an area that is ripe for further investigation. And I think there are bad actors out there that within the FTC's -- even under the harm's-based standard that has sort of dominated the paradigm of late, I think you could find instances where unfair and deceptive practices are going on.

But to point out some of the examples that Amina and Kevin brought up, I think if you think more broadly about the dignity-based standards that Director Vladeck has spoken about in recent months, I think there is an even broader base and potential for further enforcement.

One other aspect of some existing FTC authority links in tightly with the self-regulatory programs that already exist. And I kind of wonder about how those programs are enforced and what the kind of accountability and compliance mechanisms there are to back up those self-regulatory programs, because without that kind of teeth, it is not really clear whether -- if no companies are getting kicked out of the self-regulatory program or if there is actually no compliance measures that are brought to bear, then it is unclear whether the self-regulation is really actually working.

I think as far as further regulation and legislation goes, obviously CDT is highly in favor of baseline federal privacy legislation and we think that location information could be part of that framework where we think about sensitive kinds of information. I think location information and perhaps other mobile-device data could be incorporated into that kind of framework.

And, as we've spoken about earlier, ECPA and ECPA reform is another area where new legislation is absolutely warranted to level the standard and make sure that when we do get requests from the government for location information, that the probable-cause warrant is the standard that is in use.

MS. HARRINGTON-McBRIDE: Amina.

MS. FAZLULLAH: I think I don't want to sound like I am just saying ditto, but I think that are three ways that we can -- if we can strengthen user control, if we can strengthen sort of rules around requiring transparency when someone starts to engage with a company that is going to ask for this information, and then of course compliance and enforcement.

So I think what is difficult is that while self-regulation is probably the first place where you are going to see a lot of great ideas come out, because these companies can tell you what they can and cannot do right off the bat, so that is a really interesting place, I think it is important that there is kind of a leveling that's done. There are the good actors and the bad actors, and without the federal government involved it is really difficult for any of those bad actors to actually show up -- or to be found out, rather.

So that is why U.S. PIRG is also involved in improving legislation or pushing forward legislation on privacy and hoping to strengthen the existing authority of the FTC or at least encouraging the FTC to act on the authority they have already gotten to look into these problems online and in the mobile space.

MS. HARRINGTON-McBRIDE: Michael, would you like the last word on this part?

MR. ALTSCHUL: I don't know if I will get the last word, but I would like it. One thing that we all need to do a better job at, and the -- see, already (referring to Mr. Bankston's table tent) -- and the Commission needs to be congratulated for these dialogues, is education. It is part of the Fair Information Practices and it is something that I know in our association we have recognized the need that we all need to do a better job of educating consumers, particularly with technology and applications that are evolving and changing so quickly beyond what expectations of even last year would have been.

Secondly, I am in the camp that the Federal Trade Commission Act does provide enforcement authority. And if the Commission's guidelines -- for example the behavioral advertising guidelines were incredibly welcomed by our industry, an awful lot of activity had been held back waiting for some guidelines, sort of rules of the road that would allow various ventures to proceed. So more of those. They can be revised, they can be less formal than statutes.

And if there is to be an updating of statutes, obviously Congress is always aware of the fact that they try to future proof their rules. Unfortunately they're rarely successful in an industry that's as dynamic as our industry and the computer industry. So there is always a risk when Congress is in session.

The one thing that we would not endorse is a system of 50 different state sets of privacy rules, particularly for a mobile technology and Web-based technology. It becomes a patchwork quilt for educating consumers, it becomes a nightmare for not just carriers but for customers who operate in a lot of jurisdictions. The best example of course is those of us who live in the Washington, D.C. market where there are three jurisdictions, all one bridge across -- there is one bridge that is in three different jurisdictions. But with that, if there is to be rewriting and privacy laws, it should be at the federal level with future proofing in mind.

MS. HARRINGTON-McBRIDE: Thank you.

MS. LEFKOVITZ: Okay. Hang on, Kevin, I have a question for you. So what are some -- are there any other ways to mitigate privacy risks in mobile computing?

MR. BANKSTON: That is what I was going to talk about. I do not want to ditto or take issue with anything said on the regulatory scheme -- regulatory solutions: Reform ECPA. Please, FTC, help -- protect us.

But there are technological solutions as well. Many of you saw our staff technologist Peter Eckersley on the first panel today. He along with a researcher at Stanford wrote a great white paper on locational privacy and how not to lose it forever, that pointed out that there is research now into cryptographic techniques that would allow location-based services to be provided to you without the service knowing who you are.

Rather saying, 'Hi, it's me Bob and I'm here. Please tell me where is the pizza place or are any of my friends here,' you would provide a cryptographic token that would say, 'I'm somebody who is a customer of yours and not a spammer. Here is my location, please provide me service.'

So it is not actually technically necessary for all these services to know who you are. And there are technical solutions whereby we could ensure that these services do not know who you are, but this is going to require research and it is going to require investment. And sometimes it will be more expensive for the provider to provide such a safe service than otherwise. But, as we saw, for example, the last couple of weeks, Google implementing HTTPS encryption for its email, for example, there can be competitive or other political or other benefits for companies to look into these kinds of approaches.

So if you want to look at that paper just Google for EFF on locational privacy, or Bing or Ixquick or whatever search engine you prefer.

MS. COOPER: I would just add that we also should not lose sight of all the privacy protections that exist for other forms of data. They also work for this kind of data as well. And if you think about in a security context there are some Web browsers that communicate with location services, the service that actually locates the device. Firefox is one of them that communicates with its location provider over an encrypted channel. There are some that do not.

We have known for a long time that encrypting the communications channel is one way to prevent eavesdropping and help protect privacy. And yet it is kind of a baseline protection that hasn't really become ubiquitous in the marketplace. So I think there are new techniques that can be very useful. There are also very old techniques that would also help out.

MS. HARRINGTON-McBRIDE: Brian -- oh, hang on a minute. I am going to ask Brian a quick question here because, Brian, you are the guy in the business here, so let's talk to you for a minute about these potential technological solutions, cryptography, something that you think would be workable in a business context, is it scalable?

MR. KNAPP: I think there are some questions about that. I mean I think it sounds great. So, first of all, just to step back for a second, I do not know that some of this stuff is not already in place. So on the iPhone an application can know only your UDID, which is not tied to you. And you can hit their location, the API, to get a location fix. Combine that with the UDID, and you have exactly nothing in terms of who the person is, and you can provide a very robust location service.

BlackBerries has a similar approach, actually. I mean there is a device I.D., but if you were going to use that it would be actually hashed. So some of this stuff is already out there. And, trust me, that application providers aren't unnecessarily, at least the good ones and I think most of the popular services are not unnecessarily getting more information than they need to provide the service.

So I think particularly in Silicon Valley engineers, by their nature, are careful about data security and very entuned to it. And most of the popular, successful companies, I do not think it is any coincidence that most of us are taking privacy and data security pretty seriously.

So we are looking to implement a strong data-security measure balanced with what is practical. I mean the way the Kevin put it, that it would cost the provider a little bit more to do x, y, and z, well, what he is really saying is it is going to cost the user more. And so to the extent users are looking for advanced technologies to keep them private, then of course they are welcome to pay for that kind of stuff. But it is not necessarily our experience that users are willing to pay a lot more to go out of their way when some of these technologies are already in place.

MS. HARRINGTON-McBRIDE: Amina.

MS. FAZLULLAH: I guess I just wanted to add that at least on the mobile platform there is not -- when you go in the online world and using your computer, there is a lot of stuff that users can do to check who has been following them or, to some extent, to look at cookies or look at other things. And on your phone it is very difficult to be able to do that, even though you are starting to go online or you are being behaviorally targeted or tracked for ads.

And so since you do not -- again this is going back to user control, but actually I am more talking to the companies that are sitting up here, it is another way again to build trust with your customer. If you actually build in -- if Motorola has a device or if Sprint decides to allow consumers to be able to access this information and clear it out or control it, then you will have a lot more awareness and understanding and smarter consumers who are going to be just happier consumers generally. And it is another easy way of generating trust and helping people control their own privacy.

MS. LEFKOVITZ: Great. Well, I think that is our time and I would like to thank our panelists for an excellent debate.

(Applause.)

MS. HARRINGTON-McBRIDE: We are going to resume again at quarter till the hour and that will be our final panel of the day.

(Recess taken from 4:33 p.m. to 4:46 p.m.)

PANEL 5: TECHNOLOGY AND POLICY

MS. RICH: So welcome to Panel 5, Technology and Policy. I am Jessica Rich. My Comoderators are Katie Ratté and Naomi Lefkovitz, who I think I just hit, who I think are going to let me do most of the talking and rest on their laurels from earlier in the day.

Our topic for this panel is Technology and Policy. We are going to build on other panels and take it the next step, which what are the implications of the issues we have discussed for policy and for policymakers.

So I have a great panel to help me discuss these issues:

Ellen Blackler, right here, is Executive Director of Public Policy at AT&T;

Fred Cate is Professor of Law and the Director of the Center for Applied Cybersecurity Research at Indiana University;

Peter Cullen is Trustworthy Computing and Chief Privacy Strategist at Microsoft;

David Hoffman is Director of Security Policy and Global Privacy Officer at Intel;

Joanne McNabb is Chief of the California Office of Privacy Protection;

Hana Pechackova -- I got that right, didn't I -- is Policy Officer at the European Commission, Directorate-General Justice, Freedom, and Security in the Data Protection Unit; and

Lee Tien is the Senior Staff Attorney with the Electronic Frontier Foundation.

So we basically have four questions we want to consider in this panel:

First, has the market done a good job of offering privacy and enhancing technological tools to consumers, and why or why not.

Second, how are companies using technology to protect privacy? Are these efforts adequate?

Third, what can and should regulators do to increase the uptake of privacy-enhancing technologies?

And, finally, although we will entertain other topics if people are interested, how have regulations to date affected the uptake of the technologies and is regulation a good way to encourage the development and use of privacy-enhancing technologies or not, and are there better ways?

So why don't we start with the first. Has there been adequate uptake of privacy-enhancing technologies in the market? And I would like Fred and Lee to maybe discuss this at first, and then other people can join in.

PROFESSOR CATE: Thank you very much, Jessica.

And thank you again for the opportunity to be on this panel.

I think the answer, to be honest, is it depends. And so then it matters on what it depends on. So it depends on first what technologies we are talking about. And I think one of the useful discussions we have had throughout the day is what do we mean by privacy-enhancing technologies.

If we us the broad definition, the way I think a number of the panels earlier have done, so that we are including things like spam filters, auditing software, monitoring software, and so forth, then I think we would say, yes, we have seen a fair amount of pushing privacy into products and consumers and, particularly, business customers willing to pay for those. So look at the additions to operating systems, to browsers and so forth, we see a fair amount of privacy-specific or privacy-responsive technologies.

If we define privacy-enhancing technologies as I think they are more often defined in certainly the scholarly literature to mean things that consumers buy that enhance their privacy, then I think the answer would be no. We have seen a lot of efforts to do that, P3P being probably the earliest and biggest. And what we have seen is remarkably low uptake by consumers and a real unwillingness, if you will, to put our money where our mouths are when it comes time to buy privacy-enhancing technology as a separate standalone product.

MR. TIEN: Yes. I agree with Fred on that and I want to sort of talk about some of the reasons why consumers really have not embraced it. And I think probably the most important is a question of existence. Does a privacy-enhancing technology even exist for a given threat.

One example that has come up during the day is, for instance, the question of, say, certain kinds of supercookies like Flash cookies. For quite a long time there was simply no available kind of plug-in for most browsers that could even be used for it.

Aside from existence, then consumers actually have to perceive a threat of some sort and have knowledge about it even to seek out the use of a privacy-enhancing technology. On the tech side, many users do not know anything about these threats. And we actually had an example in the mobile panel just now about how, well, what do consumers know about whether or not their GPS can be pinged or not.

On the legal side many users falsely assume, according to recent research, that their data is legally protected by the existence of a privacy policy anyway.

So, again, you might think, well, if you think the law protects you, then do you need to get this tool in order to actually protect your privacy.

And then a third reason really is the inconvenience. If you are not getting your privacy-enhancing technology as part of your browser and on by default, you may have to as a consumer go through installation steps and then actually endure inconvenience when you are using the Web because, as we discussed in the first panel, many of the tracking tools that are threatening privacy are actually part of the way the Web works. And so when you don't use Javascript or don't use other kinds of tools, then you are also possibly not going to be able to use Websites that require them.

MS. RICH: Lee, you said that tools just aren't produced so consumers can acquire them. But it is sort of a vicious circle. That implies there is no demand for them. But do you have another explanation for why the products are not out there available on the market?

MR. TIEN: Well, I mean I think there are a number of reasons. First of all, you need to -- you know producing software, producing a tool costs resources. So what is your business model for producing that? We have seen a lot of tools that are produced, say, by I guess I would call them altruistic programmers or folks who decide that they want to build this sort of tool in order to, say, promote anonymous browsing. You know EFF helped support a tool called Tor which is an anonymous browsing tool. It actually had been originally subsidized by the federal government as part of the Office of Naval Research. And because it got some kinds of nonmarket support, it actually still exists out there and is fairly widely used among privacy-enhancing technologies.

But I do not think that it really makes sense to think about how the market is going to produce those independently of larger equipment manufacturers, whether it is the browsers or OSes or whatever. These small shops, it is not clear how they are going to get paid. They are not going to be relying on an advertising model the way a lot of other enterprises on the Web are.

MS. RICH: Ellen, are you going to address the demand or the availability?

MS. BLACKLER: Yes. I just wanted to add to what Fred and Lee said. Another barrier is that one of the things we are coming to understand is that the threat is not perceived uniformly, that one person's threat is another person's benefit. So where in virus protection and malware there is a pretty universal understanding that people do not want that stuff, and so the virus -- there was kind of a uniform big block of demand that.

And now you see, 'We do that on our network because that is what our customers expect.' But you do not have one way people are viewing these privacy threats, so what you have got is a bunch of fragmented demand. And I think that is another factor.

And really I also wanted to underscore this transparency issue, because we spent a lot of time talking about transparency as a solution. I think it is important to recognize kind of the exponential benefit of that, because through transparency people then understand if they think it is a threat, they feel threatened, they start demanding more. And that is this virtuous cycle.

MS. RICH: Peter.

MR. CULLEN: So this is the right process, my tent is up; is that right?

MS. RICH: Oh, yes, you are following the rules.

MR. CULLEN: Good.

MS. RICH: You are following the rules.

MR. CULLEN: I liked Fred's parsing of the definition. And I think it is a really important question, because if you think about the, I'll call it, the true disciplinary definition of PETs from, I'll call it, a European perspective, it does get into this enhancing mode, which I think Lee touched on a lot. But what I also heard from Lee was a discussion about or questions about the effectiveness of this.

I'm not sure that the metric of market adoption is necessarily the right one and I think there was a comment made earlier that the fact that these tools are available actually promote trust. And that is a different thing than saying that they are only effective if people have taken them up.

And I would argue that even the opt-out method is, by Fred's definition, some form of privacy enhancing. The fact that very few people take advantage of the opt-out is not a metric to say that the market has failed, it is a question to say that I think that consumers value the availability of these sorts of privacy enhancements that do not necessarily feel that they have to take advantage of it.

MS. RICH: Hana.

MS. PECHACKOVA: I would like to share our experience from the European Commission point of view. We have launched a study on economic benefits of privacy-enhancing technologies. We are somewhere in the middle. We have the first interim -- the second-interim report, and there were quite interesting lines why that did not really take up yet and what are the major problems.

It is not about threats only, it is more about information sharing, about information failures. Because companies, they tend to withhold the data, not to really inform the public about breaches of laws, about the data leakages unless they really have to, unless it is a legal obligation. So that is why we are looking at the possibilities to introduce into our law the obligatory notification of a data breach. Because if you really see clearly that there were cases, and there are cases, it is happening every day, that there are cases, then there are some leakage of data, of course you would have a very, very good business case for deploying privacy-enhancing technologies, for really taking it seriously and looking at that. It is not only about threats, but you really have to see that there are problems in practice in everyday life. So this for me is one of the reasons and it has also been confirmed by our researchers.

MS. RICH: So it is transparency not just on the consumer side but on the business side?

MS. PECHACKOVA: Exactly, yes.

MS. RICH: Lee?

MR. TIEN: Yes. I just wanted to add a couple of meta points. I mean one is that I don't think privacy-enhancing technologies in sort of a market-adoption area is really going to be a particularly powerful answer to consumers' privacy problems. It is not that they are a bad thing to have, but I don't think that you are really going to protect the privacy of the vast majority of the public with that.

And part of that I think is simply the same kinds of problems we have been talking about all day with respect to consumer choice and the ideas of transparency and how you frame the value of these things. I mean you can frame them in terms of 'We want to give the consumer a choice, be able to decide what to do,' and that is sort of an individualistic, atomistic perspective on it. Or you can frame transparency and choice and access more in, what I want to think of as, a model of facilitating social oversight, right. It is not necessary -- the idea is not that we are going to reach these thousands of individuals.

What we are talking about is that we are going to have information that is transparent so that those who are privacy sensitive will be aware of it, NGOs that are involved in privacy advocacy will know about it, the regulators will know about it, and we will be creating really an enforcement sort of feedback loop with that kind of information. And that is the way I think of a lot of these kinds of transparency goals. It is not really for the purpose of enabling each consumer, although certainly they have an entitlement to some of this information, but really to make a larger enforcement feedback loop actually work.

MS. RICH: Thank you.

Fred.

PROFESSOR CATE: I would certainly echo that point and, frankly, would also go back to an earlier point that Lee made, and then Hana's comment made me think maybe was worth coming back to accentuate, and that is one of the reasons we may not see market take-up of sort of traditional privacy-enhancing technologies is because there really are not technological solutions to a lot of the privacy issues. That it is a mismatch, if you will.

And Hana's example of security breaches made me think of this entirely. I cannot imagine why security breaches would motivate more consumer take-up of privacy-enhancing technologies given that security breaches involve companies that typically lawfully have the information, need to have it, or have it for a reason. There is nothing I can do. I can buy all the privacy-enhancing technology I want, put P3P on, set all my browser settings. Nothing is going to help me in that situation.

So the traditional view of privacy-enhancing technologies would say they are just useless in terms of the types of situations that I think today has helped kind of hone that people really worry about. We have a good example here. I mean we have had a notice of security breaches of course in California for four years now -- well, how long has it actually been in effect, has it been seven?

MS. McNABB: Seven.

PROFESSOR CATE: Seven. So we have the expert here.

Yet we do not see California running out to buy privacy-enhancing technologies. There has been no tremendous P3P upsurge here. Not because -- that wouldn't be a rational response to that. And so I doubt if we are going to see privacy-enhancing technologies picked out as an irrational response to these types of threats.

MS. RICH: Well, what you are talking about, though, is a good reminder that, and Hana's remarks too, that privacy-enhancing technologies are also very important on the business side, if you think of them more broadly. And I think -- David has his tent up and he is also well situated to answer this -- how are businesses doing using technology to protect data and how are they ensuring that it is used at the earliest opportunity so that it is not superimposed on existing systems so that it becomes extremely expensive to incorporate?

MR. HOFFMAN: Yes. It is never a good idea to disagree with Fred, actually, so I try to phrase this carefully, that I actually would agree that I do not think we have seen a huge uptake because of individuals receiving a great number of security-breach notifications, that they are reaching out and saying, 'I am going to spend more money now on privacy-enhancing technologies.' Although you might be able to stretch the example a little bit to say the awareness of cybersecurity as a problem has increased the likelihood of people keeping their antivirus software current and actually paying for that, which I think the numbers are greatly increased that people actually try to do that.

I do think that -- Jessica -- you are right on the enterprise side. There is a much better case to be said that the encryption safe harbor and many of the state security-breach notifications statutes has played a tremendous effect in getting companies to deploy encryption technology in a variety of different settings, whether that is in transit or, more likely, in storage. And where I think we are seeing it a lot is on laptops and other mobile devices now, to better protect the data. And that is a great role the regulators play in spurring people to do something that was really the right thing to do.

MS. RICH: Well, so besides encryption what are you doing to protect data?

MR. HOFFMAN: Well, that is an interesting question. For us a large amount of the data that we have, right, is the data we are storing on our backend servers in our enterprise systems. So this then 'What are we doing to protect data' gets into a large discussion about what are we doing for cybersecurity. It is not just about protecting personal data but it is about protecting our intellectual property and the data that we use to run our business.

I think there is a tremendous amount of investment going on across the board for companies there and a tremendous amount of investment of trying to intersect development life cycles -- I know we are going to talk about this a little bit later -- but to do that earlier and earlier so you are not bolting on things later. And I know that has gone down to the vendors, that the vendors who make this enterprise software, for example, are baking that in.

It happens at the hardware level for the things that we produce and I think software vendors would say, could talk about the tremendous investments that they are putting in and protecting that data.

MS. RICH: Well, I do want to talk about baking it in at the earliest opportunity. Peter, are you prepared to talk about that?

MR. CULLEN: Yes, I can.

I just want to make sure, Lee, do you want to continue on this point?

MR. TIEN: I wanted to throw in one quick point. And, again, it is like the point about notice of security breaches and what Fred was saying, at EFF we are always recommending to folks if you don't have the data you can't be forced to give it to the government and you can't leak it or anything like that. And having the opposite of data retention, data deletion as a policy, as a practice is something that, you know, really doesn't require any fancy new tools. It is just something that people could do, would be very cheap, and would mitigate a lot of privacy problems. And we need to think of incentives, more incentives for doing that.

MR. CULLEN: So I think there is ample evidence over the past decade, to even 15 years, to suggest that, well, there is a market in the customer's face for what I will call true privacy-enhancing technologies. It is a relatively small one. Whereas what has happened over the past four to five years, particularly in the business case, is a much greater demand for privacy or data protection type technologies or informational governance type technologies and solutions. So certainly as a provider of those sorts of things, we are seeing a great demand for that.

But I want to introduce kind of a third leg to Fred's split, and I think it is at your question which I will call: Privacy-enhancing processes. And I think this is a pretty important thing for virtually all companies to think about.

I think there was a discussion earlier around that. And I must admit I found myself thinking that our business must be more complex than that particular company. What we found is while obviously very prescriptive and descriptive policies are superimportant, they actually do little to provide guidance to an engineer as to how to design privacy into the product.

And so the experience that we have had is that requires almost translating a policy into, I'll call it, geekspeak, where it becomes very code like in terms of what we mean when we say provide consent or provide notice when a certain data is being transferred.

And the solution from at least Microsoft's standpoint was to be very prescriptive about these standards and to build them literally into the software development lifecycle so they become part of the way the company does business. Our previous model that I am talking about even sort of six or seven years ago of perhaps relying on lawyers to review products as they were going out the door really just did not prove to be very tenable.

So this way of designing into the process allows for, I'll call it, the stated objectives to be met.

I think the other kind of maybe splitting back into the privacy enhancing for the community was simply to make those standards publicly available and to start to build them into other lifecycle type transparency communication things, making them available for other software developers, the way that we have thought about it. So this really is a complete but very prescriptive cycle, at least from Microsoft's perspective.

MS. RICH: What are the incentives for companies to have more privacy-enhancing products? I think in many ways we are also talking about defaults, --

MR. CULLEN: So --

MS. RICH: -- which was the subject of a lot of discussion earlier.

MR. CULLEN: Yes. So I think there is --

MS. RICH: And what are the disincentives too?

MR. CULLEN: Yes.

MS. RICH: I want to get at both.

MR. CULLEN: So Microsoft is perhaps different from other companies in the sense that, like all companies, there is an expectation that we have robust protection around and appropriate use of information, but I think that where the difference is that consumers and businesses expect us to provide them with technology that helps them protect their information. So I think there is a different motivation from Microsoft's standpoint.

I think the fact that we do not have -- you think of kind of an operating system, there really is not a direct relationship with a consumer. There is an arm's-length relationship. It means that the trust perception, the trust relationship is much more difficult to obtain. So from our standpoint the onus is to be that much more trustworthy in there.

I think the other advantage that kind of we have found from our experience of building it into the development lifecycle is it actually generates privacy-enhancing capabilities. And I will use an example of a review on the phishing filter.

And the model was, wow, in order to provide dynamic protection from phishing, we need to collect IP addresses from users simply because the market of phishing is just so dynamic that is the only way to do it. Well, it probably stands to reason that many people would feel pretty uncomfortable about sharing their IP address with Microsoft, even if it was for only the purpose of providing phishing protection. The answer was to simply separate the IP address out from the path, delete it immediately, in order to provide the consumer with the protection. To be very clear about that; in our case, actually had that audited. So I think there is an example of it went beyond what I'll call our standards were, but it was a way to provide that added level of trust for the consumers. I don't think you can do that unless you bake it into the company's process.

MS. RICH: David, can you talk a bit -- and actually Hana got at this a little earlier, which is some of the exposure that companies have from breaches, has given them an incentive to incorporate privacy-enhancing technologies, but can you speak to some of the incentives and whether maybe those have changed in recent years?

MR. HOFFMAN: Yes. Let me try to speak to some of the incentives and disincentives, if that is okay?

MS. RICH: Yes.

MR. HOFFMAN: I want to build on what we heard in the last couple of panels also. I think in the last panel we heard this concept of that there are these ideas that there are going to be these brands in the future that you are going to feel that you can trust. And that is almost your gateway into receiving certain services through certain technology.

But then I think what we also heard on the cloud computing panel is that really that is not just a brand but that is almost a sphere of trust. You are depending upon a brand or a company to make sure that everything within a certain sphere can be trusted. So I think we are seeing more and more from a brand perspective there is going to be that incentive.

I think there is also we are increasingly seeing disincentives coming up in individual situations. Let me give you one example that I think is a really good example.

So at the end of 2005 the Federal Financial Institution Examination Council, which is for those who do not know, a multiagency organization of the federal government that includes the FDIC, came out with a guidance document expressing dissatisfaction with the idea that there would be online banking that would be done just with a single factor of authentication. So generally they are thought of as three different factors of authentication, things that you know, things that you have, or things that you are. And most online banking experiences up to that point were primarily just things that you know.

And so what was interesting about what they did was they, through this guidance document, sent a message saying: Get better at this or there is going to be some substantial disincentives for not having better tools here.

What I think is particularly interesting about that is the effect that that has had throughout industry. So the banks then went to the folks who provide the authentication services for them and said, 'We're hearing this; we need better tools for doing it.' Those companies then ended up coming to us for hardware, other software companies saying, 'We need better privacy-enhancing technologies.' And now what we are finding as a result of that, that we have got projects pretty far along coming out of our labs at this point to provide some very good hardware-based, and I know there is also software-based, further methods of authentication.

So I think that is an excellent example where you have got the trust on the one side working as an incentive, but then selected disincentives that come from regulatory agencies or quasi-regulatory agencies to create even the specter of the disincentive, which pushes things along.

MS. RICH: Okay. Well, Joanne, you have got your tent up. Do you want to -- are you going to address the incentives and disincentives? Sort of.

MS. McNABB: I think so. Yes. Yes.

Just building on what David said, his mentioning the authentication regulation ultimately, but first just raising the issue. In a way that same approach is what the breach-notification laws, it is the way they have operated. It did not say you have to use these things to protect information. It said -- it created, it revealed a price, the price of having bad security, bad privacy practices, and it shifted the burden of paying that price from the victims, whose information, as Fred said, they could not have done anything to protect, onto the party that could do something.

I think one of the reasons that the market, one of the factors in why the market has not kicked up more PETs, is that that sort of -- the actual costs have been hidden, the costs to consumers have been hidden in many cases.

MS. RICH: Hana.

MS. PECHACKOVA: I would like to briefly talk about incentives, but about the role of the regulators, because it is up to us, the regulators, to show that they are not --

MS. RICH: We are definitely going to get to the role of the regulators, but I just wanted to sort of finish up with more the businesses' own incentives, even outside of regulation. Everyone is dying to talk about regulation, which is very interesting. He's bursting out of the crowd, even the companies. But...

MR. CULLEN: Let me take an I-agree-with-Joanne-and-I-disagree-with-David scenario. I can disagree with David, but I do not disagree --

MR. HOFFMAN: Yes.

MR. CULLEN: So in order for there to be this, I'll call it, perfect alignment, we need to think about market forces, social and economic. And here is kind of a real-life example of it.

We could dramatically reduce the identity theft at least in the credit card stamp by having keyboards that were able to read magnetic stripes on keyboards. When we go to the manufacturers of those, we say, 'Well, why don't you produce a mag stripe on that?' Well, the answer is that a consumer is not prepared to pay $15 more for a keyboard for a mag stripe. okay. So we go to the store -- and, besides, there are no online stores that are capable of receiving this.

We go to the online stores and say, 'Well, you know we could actually reduce the threat if you had the ability to read mag stripe read cards,' and they said, 'Well, no, because consumers do not have the keyboards and the cost of rebuilding our infrastructure is just really prohibitive for us to do that. And, besides, right now in an online transaction, the cost of the fraud is actually born by the bank, not by us.'

So we go to the bank and say, 'Well, why don't we do this,' and they say, 'Oh, well, actually, no. If we do that, it actually makes it a card present and that actually might move the liability really, really to us, so there is no real motivation for us.'

When we go to the regulator and say, 'Boy, you have got this industry and guidance about two-factor authentication, why don't you use this as an example. It would have such a dramatic impact on this,' they say, 'No, no, no, we can't interfere in the market.'

MR. HOFFMAN: So I actually don't think you are disagreeing with me. I think we agree, which is there is a role for the regulators to play to encourage the things that are fundamentally broken and that that plays a great role within the market.

MR. CULLEN: I am relieved because I do not like to disagree with you. That is good.

MS. RICH: Okay. Well, we got to go to the regulation because that is what everyone wants to talk about. I know these guys have things to add on that, so why don't we talk about what is the role of the regulators in encouraging the uptake of these technologies both on the business side and to offer to consumers. So, Hana, I know that you have spent a lot of time thinking about this. You have done a lot of work with the European Commission to promote privacy-enhancing technology and privacy by design, so can you talk a bit about that?

MS. PECHACKOVA: Yes. Sure. The European Commission did a lot of work in this field. We did a lot of research. We invested lots of millions of euros into the research. We did it together with our colleagues from Direct Regional Information Society and Media. The research in this field started, if I'm not mistaken, back in 2002. It was under the Sixth Framework Research Programme. They were interesting studies and interesting research, like PRIME or FELIS (phonetic). Now we are running the Seventh Framework Programme, and again a lot of millions of euros are invested. But it is not only the research of the European Commission, it is usual there are public contenders and we are working together with industry on how to get it right. But we are also launching some other studies to look at the policies, what we can do to bring the privacy-enhancing technologies into policy and how to regulate, whether we should introduce it into new laws or not.

It took us some time to create in Europe to build our democratic values, it took several generations, but now with the new technologies of course you have to foster those values and bring them to the digital era, to the digital age, but how to do that.

So we are currently looking at the future of privacy, the future of protection of personal data in the EU. In the last year, in July 2009, we have launched and brought online public consultation. And the EU received very good feedback. We received more than 160 replies from individuals but also from associations and from companies. So one of the lines were that we have new technologies that are challenging our values, but we could also use some of those technologies to help us, because you cannot address everything only in the law. So the technology could be kind of a complementary mean to help us to get it right.

So we have to be innovative and we are looking at what to do because we do not want to step back of course from our values, but we have to make our legal regime more workable and more adjustable to the current situation. So ideally we would introduce new principles which would be, for example, the principle of privacy by design, which is one step ahead of the privacy-enhancing technology. So we would absolutely support that. That then would be privacy-enhancing technologies but in a broad sense of course, because when you have privacy-enhancing technology you have kind of two phases of that.

The first one is before you implement you think really twice. And then when you already implement the technology and then after that you embed some enhancing tools into that. So we also wanted to supported this by the study on the economic benefit, because it's our role, the role of regulators to give incentives, that we just talked about. And we want to show of course -- you mentioned trust. Trust is of course the backbone of the information society. And the data are circulating by business every second around the globe, so this is very important for us. It's not only about trust, we have to show that there are economic benefits. And if there are economic benefits, we would make not only companies but also public sector to use it because we are looking not only at the private individuals or at the private company, but they are also looking at the government level.

It is also very important that the government, the public sector implements the privacy-enhancing technologies because the trust in there would really give uptake of all the economic applications, it would help to save money again for the public sector. And if you show the incentives it will be of course ideal situation.

And then on other principle would be the principle of accountability, but we can take long hours about accountability.

MS. RICH: Thanks.

Joanne, California's been in the forefront of privacy and security regulation. Has there been a focus on encouraging privacy-enhancing technologies either in your state or others that you know of?

MS. McNABB: Not that I know of. I think there has been some impacts in that area, but not necessarily intentional, apart from the extent to which the data breach notice law resulted in encouraging encryption, for example, or data loss prevention software.

I think one of the earlier laws that definitely produced some privacy-enhancing -- or encouraged privacy-enhancing industry was the statute in 2000 in California that requires companies to render records containing customer information unreadable before disposing of it. And that ultimately has worked its way, that idea, into the disposal -- the FCRA disposal rule and it seems to be sort of implicit in HIPPA and GLP, but in 2000, when my people from my office would go out and speak to groups of consumers, it was usually at legislator meetings, for example, who were coming to hear about identity theft. So these were privacy fundamentalists or privacy-activated people. And we would ask them questions and have a raffle and give away a shredder at the end. And, oh, they were thrilled.

Well, after about two years everybody already had a shredder. So I mean the consumer uptake definitely occurred. And there is a whole industry that is not called the shredding industry, it is the information-destruction industry that goes from shredding papers to crunching up and recycling computers and beyond, and does a lot of education on the laws that require you to do that.

MS. RICH: And you supported those laws.

MS. McNABB: Yes, indeed.

MS. RICH: So, Ellen, to what extent has your company and others like you been influenced to adopt privacy-enhancing technologies because of regulation, or not?

MS. BLACKLER: I was going to talk about the kind of conundrum we have got here is that it is hard, it is a really complicated ecosystem, it moves very quickly, you do not want to set something prescriptive because it screws up with the innovation, and so the temptation is kind of to throw up your hands. But I think that we have seen some success. You guys put a pretty big spotlight on behavioral targeting over the recent past and put out the self-regulatory guidelines.

And I think not to overstate any of that, but the industry kind of hopped to. And I think we have seen over the last couple weeks with the National Privacy Day and the workshops these announcements about things that maybe are not going to solve the problem but took cooperation across a range of folks in the ecosystem that would not have had happened absent the spotlight you shined on it. You know, the icons that will now be used in advertising that will start to get at the technology. I think the introduction of the profile managers by some of the big ad network companies. You know all of that is because of the spotlight that the regulators shined on it, which then made, I think, consumers wonder what was happening. And the combination does result in a focus on privacy.

Now we at AT&T are not in the ad network business really so much, so we do not do too much of that. But where we did enter the business we made sure that we had a profile manager and we had separate notice and we had these kind of what we call table stakes to get into the business because you guys said these are table stakes, get into the business.

So I think that is an important way to balance, to weave through the need to not be prescriptive but also have something. The privacy by design I think is another emerging issue that is going to be hard for a company in the near future to not have an answer to what is your internal process for making sure privacy is considered. And some of that comes from the regulator saying, 'This is what we expect, this is the best practice.'

I know sometimes the self-regulatory best practices are kind of pooh-poohed. But whether or not you support legislation, whether or not we can agree on legislation, that stuff is going to have to happen, even to figure out what the legislation should be. So I think we should not be distracted by what the legislation should say and not work on -- kind of do the work to figure out what the operating best practices are.

MS. RICH: Does any regulation or self-regulatory standard that promotes privacy tend to promote privacy-enhancing technologies or -- because behavioral advertising, the principles, weren't specifically designed to promote privacy-enhancing technologies, but that is what they have done because of the nature of the space they are addressing. But does that happen with any government action or are there different ways to focus in on -- to encourage privacy-enhancing technologies, are there things that people can do right, government can do right or the things that government can do wrong?

Oh, people are putting their tents up. That's good.

David. Ellen, did you want to address that?

MS. BLACKLER: Go ahead.

MS. RICH: Okay. David.

MR. HOFFMAN: Well, I do think not everything the government could do would be the right thing to do. Just to echo something that Peter said earlier as way of illustration, because it's proven, almost the exact same story.

When we started our privacy-review process internally we repeatedly would have this issue where the trigger in our development lifecycle would have the engineers come talk to the lawyers, which is usually me at that point, and they would say, 'Where are the legal requirements? Can you give them to me? I just need to know how to code this into the product. Just send me the requirements.'

We said, 'Well, you know we are really talking about reasonable choice and control, and figuring out what that was.'

And they would throw their hands in the air, saying, 'I can't code reasonable.' And then they're jumping -- there would generally be two or three lawyer jokes thrown in as they swore under their breath.

But then the reply that I got good at giving after a while, after I thought about it, was to say, 'All right, do you really want the lawyers designing the product? Is that what you're really' -- and the answer was really no, but the engineers were actually pretty good at solving problems if you give them the problem that you want them to solve and you provide them with some freedom to figure out how to do that. And I think that's been the direction where we have seen regulation that has moved in the right way. It is regulation that has said: Here is a problem and this is unacceptable. We are not going to give you the exact answer of how to solve this, but if you don't solve it there is going to be consequences associated with not solving it.

MS. RICH: So the ultimate standard, but not the way to implement the performance standard, but not the way to get there through by mandating specific technologies?

MR. HOFFMAN: Well, and I think underneath that we could talk about -- because I don't want to take too much time because I --

MS. RICH: Yes.

MR. HOFFMAN: -- know other people have comments, I think underneath that then you have relationships between the regulators and industry and academics and NGOs about how do you provide guidance underneath that so that David Hoffman's not talking to the engineers and trying to make up all on his own what he thinks reasonable is. But that is not necessarily part of the regulation. We talk about that as a sort of triangle of trust with those entities coming together to figure out some of those problems.

MS. RICH: And consumer.

MR. HOFFMAN: Indeed.

MS. RICH: Lee, do you want to address this issue?

MR. TIEN: Yes. I just wanted to jump in and sort of -- while we have been talking about government's role here as sort of a regulator that is attempting to protect privacy, we just cannot forget that there are a lot of roles the government ends up playing that are actually pretty harmful to privacy. The U.S. government has just historically discouraged encryption technology deployment in the United States for a long time.

We have seen that there are technologies that are being deployed by local governments, state governments, as well as the federal government, such as

RFID, that are almost designed to expose information about where people are. Right now in California we are looking at the expansion of the Fastrak RFID-based toll transponder system which is not only insecure but relies essentially on a system that is going to be tracking people's location at least as they are crossing toll bridges and any other points where sensors are.

And what is ironic about this is that we know that in the EU people are looking at very interesting private tolling methods. We know that commercially available there are crypto-based systems where you can do this kind of automatic tolling with complete anonymity. But trying to get, say, a state agency like CalTrans to even sort of notice this or to get this sort of truly, I think, designed-in privacy into these systems is not an incredibly easy thing.

The third example I will use here is, again, data retention, right. I mean we have all recognized that deleting data protects privacy. And yet again the federal government is actually -- very often law enforcement will tell carriers in the telecommunications world, 'Hand over data. Keep data.' It is not clear whether or not it is actually even useful for law enforcement for data to be kept for six months or two years, or whatever.

We hear that after 30 days probably is really most in the utility of it, and yet if the government is requiring that or inducing private entities to keep data much longer for their own purposes, again that works at cross-purposes with what we are talking about here.

MS. RICH: Fred, can you address this issue of how regulation interacts with -- or regulation or nonregulation interacts with privacy-enhancing technologies?

PROFESSOR CATE: I could certainly try, but I do not want to disagree with anyone who has gone before because we are being such an agreeable panel. Well, in fact I do not disagree with much that has gone before. I think one of the things that matters a great deal really is to eliminate the disincentives point.

Or maybe a better way to think of it is to be aware of the incentives being created. So, for example, and I think Joanne alluded to this point, although we may view this point differently, we're all chasing Social Security numbers now. We are running software to detect Social Security numbers. Well, that's great. I mean there's nothing really wrong with that. It is not doing a lot to enhance the overall management of information in most institutional environments. And so I would call it, on the whole, sort of a little bit a side show, that we have taken -- because the lawyers have been told to worry about Social Security numbers, and so the lawyers have translated that through into business processes when the real message if we were going to send a regulatory message, should be: Worry about the management of sensitive data, whether that's personal or other types of sensitive data so that you can all sorts of disincentives that are necessarily bad. Maybe "disincentive" is the wrong word. But they're just tangential, they are taking us away from the core focus.

I think a second point is we need, and I understand this is the whole point of these workshops, so I am just stating the obvious and I want credit for stating the obvious, we need a little more clarity on what are the objectives.

In other words, nobody wants the government promoting a specific technology and I'm sure the government doesn't want to do that either. It will be out of date by the time -- but what we need are very clear objectives. And so security, and I think this point has been made clearly, but again it is worth echoing: That is clearly an objective I think we all agree on. And, therefore, some notion of accountability, of liability, if you have data and you do not secure it so that it is used in ways that cause some form of harm, and we can debate what that means, that that will be one way of really creating incentives for institutions to do what's best to protect the data, whether that is buy new technology or whether that's not collect the data in the first place or whether that's retain it for less time. I don't think you really want the government to judge that. I think what you want to do is give clear objectives and penalties if you don't achieve them or incentives for achieving them.

I am a little hesitant just in general about the idea of using law to promote privacy-enhancing technologies partly because they failed so miserably in the consumer market. It is a little like we're going to make consumers buy these things, when we think about it this way. And you know there have actually been some fabulous technologies out there, technologies I don't think we have talked about at all today.

For example, anonymous-shopping technologies that would let you use your credit card anonymously, would let you ship to an anonymous drop address, so that you could do the entire chain of online purchasing without ever identifying who you really are. Cheap, affordable, technologically rigorous technologies. Nobody wanted to pay for them. Consumers didn't want to, banks didn't want to, the Post Office didn't want to.

Nobody wanted to pay for those.

So I don't think we necessarily want the government saying, 'That was a mistake. The market should have worked. We are now going to make you or incentivize you to go buy this technology.'

On the other hand, there is a lot the government can do to make technology work better. And I have thought about this all day while we have been talking about anonymization and deidentification, and so forth. In most areas of law outside of this sort of privacy area, deidentification is paralleled with very strong laws.

So, for example, FDA research. If I do research I have an identifier for every research subject. And if I inappropriately link those -- it's easy. I can just go get it and compare them. It's not that it's technologically hard, it's that it's a felony to do so, and that law is enforced rigorously. So that's a law that backs up a technological process, anonymization or deidentification. And I think that is quite a useful way to think of law.

The last thing I would say and then I will just go home and you will be done with me, is to think about the roles other than regulation. And I think Lee was really making this point. The one, I'm of course the academic on this panel, I always think of as fund research. I understand the FTC is not likely to go out and establish a multibillion dollar fund for research on privacy-enhancing technologies, but we do have a problem in that a lot of the research that the government does fund, largely through the NSF in privacy, is not focused on anything applicable.

You could take it all and add it together and say this will never make one bit of difference in terms of enhancing privacy. It is fascinating research. And I live off that money. I am not encouraging us to get rid of it. But nobody -- I mean those projects are not reviewed on the basis of will these make a difference, they are reviewed on the basis of will they advance the state of knowledge.

But another role the government can play, and again I think Lee was getting at this, is by using privacy-enhancing technologies, so that if the government said we are going to go in the market for certain types of privacy-enhancing technologies, that would be probably the greatest incentive the government could create, rather than saying, 'We're going to regulate for it' or 'We're going to fund the development of it.'

Thank you.

MS. RICH: Well, I do want to comment, though, that just -- I mean we have talked earlier about why there hasn't been an uptake of privacy-enhancing technologies on the consumer side. There definitely appears to be on the business side in that you are using technology to protect data.

But you could get -- I am sure somebody could give you an argument that its failure in the marketplace does not mean there is no demand for it, that this could be an area of market failure, that you had to mandate -- the law had to mandate seatbelts -- see, now maybe I will get you all exercised. But does anybody want to give him that argument?

Hana.

MS. PECHACKOVA: It's a kind of circle because of course the consumers, they will not start using the privacy-enhancing technologies or buying them or putting them on their computers unless they would hear from us, from the regulators, that it is a good thing to have. And the companies, they will not invest into privacy-enhancing technologies unless they will see that there is really a demand for them.

So we have to start somewhere and we have to address these issues. We have to do lots of awareness-raising. We have to educate both consumers or users, individuals, but we also have to educate companies, but we have to find incentives, I would say, more for companies, why to deploy and use them in their business processes. I think this is very important. But it's kind of really a circle, so we have to start somewhere.

MS. RICH: Joanne.

MS. McNABB: Well, I think as Lee said a while ago, one of the reasons he believes the market has failed to produce a wonderful array of PETs for consumers is that they are -- what has been produced and why there has not been a big uptake, what has been produced is not conveniently available. Well, isn't built into the browsers, et cetera.

Well, wouldn't it be one of the factors here in the marketplace that the business models of much online business is to increase the collection of personal information, that there is a disincentive to facilitate people being able to do more things without providing personal information, which is a kind of privacy-enhancing technology that is different from protect the information once you've already got it from people. It is antithetical to the business model.

MS. RICH: Peter.

MR. CULLEN: I thought you weren't going to pick on me, because my tent was up and you are worried about me misbehaving.

MS. RICH: I am alternating between differing viewpoints.

MR. CULLEN: Oh, okay. So I think your market question is a really interesting one, and let me pick on two of your examples, just to illustrate this.

You used or raised the specter of seatbelts. So it has been a law in certainly most states if not --

MS. LEFKOVITZ: The initial point was consumers would not pay extra for seatbelts, right, so the government -- and so car manufacturers said, 'Well, we're not going to put them in because consumers won't pay extra,' now government had to regulate, so --

MR. CULLEN: But it is an example of --

MS. LEFKOVITZ: -- it's all bundled the price.

MR. CULLEN: It's an example of where you have a law that says you have to wear it. There's been, for 20 years or so, there's been an incredible amount of education.

The downside of not wearing a seatbelt is pretty real: You die. Yet still only today 80 percent of Americans wear seatbelts.

Antivirus. There are huge business models. I mean there's huge companies that make business out of this. It comes as part of your PC as a free service. Still today 30 percent of consumers are only running active antivirus. So I think we have got it recognized this is a multifaceted problem.

But I want to get back to the technology-policy reasonableness question because I think this is where part of the problem exists. To Fred's point, technology policy will inherently fail, for lots of reasons. One is that it's complicated. Two, that the technology solutions are often outdated, and they're really fixing a very small problem. I think this gets back to even -- as I was reflecting upon the conversation throughout the day, we are doing this deja vu all-over-again model where we find an issue, whether it be social networking today, whether it be Flash cookies tomorrow, whether it be RFID yesterday, and we continue to have this debate about what technology solutions might be available or what regulation is needed.

We are not having this conversation under the banner of a framework, and let me use data-breach notification to illustrate this. Many people would argue this is a successful piece of legislation, but it's akin to thinking about what do we do with the horse once it's left the barn. Nobody has actually thought about what are the standards that help secure the barn. And when I say standards that help secure the barn, it strikes me that one of problems we have is that we need to vacillate between this prescriptive versus descriptive manner. And I think this is to Fred's point.

The BT guidance has actually been a pretty good example of a descriptive motivator that helped the industry come together and think of actual solutions to this. When you get prescriptive, it becomes problematic. But I think to say stop at the reasonableness standard, that's just not good enough because that leaves just too much open. So be more descriptive, I think, is the potential solution to this, but within a framework.

MS. RICH: So if reasonableness is too high and --

MR. CULLEN: No, reasonableness is too vague.

MS. RICH: Too vague. And then a very specific standard around a particular technology is no good, is something -- what if you mandated privacy risks assessments, is that coming in at the right level? What if you had a standard like data minimization, could technology -- would that spur technological solutions to make sure you are not keeping or collecting too much data and keeping it? I mean at what level are we talking about?

MR. CULLEN: Let's -- let's actually --

MS. RICH: Maybe Lee. Maybe -- yeah.

MR. TIEN: I guess, I mean, I love the concept of privacy-enhancing technologies, but what I care about is enhancing privacy. And I don't care whether it's with technology or regulation or with some other kind of regime.

And I think one of the reasons why we dance around the standard is because it's a very hard thing to actually sort of work out, what would be optimal. And that is the sort of thing that privacy advocates will fight -- will all be fighting about it. And it would take time to work out.

But I think that what's -- I guess I don't have a whole lot of stomach for the idea of sort of having our privacy be on in that kind of a process when I think that what we need to think about is liability rules and enforcement.

You know we spent a lot of money -- or a lot of time thinking about what the rights, say, of privacy and security rules were for health information in HIPPA. And they might be very good, I don't know. But what I do know is that for quite a few years and HHS received tens of thousands of complaints of HIPPA privacy violations, and I think acted on two.

It does not really matter what standards or rules we come up with if we do not actually have a genuine commitment of resources and political institutional will to enforce those standards, and I think that's going to -- that's going to have to include in our system actual civil liability through private rights of action. You know Paul brought that up and I think that that's a part of your ingredient.

I mean in my view one of the most effective privacy laws of all time, although that may not be so true anymore, had been the Wire Tap Act. The Wire Tap Act was a law that made very clear that the act of intercepting electronic or wired communications was unlawful. You did not have to prove harm, you just had to show this bad behavior occurred. It has -- you know Congress authorized -- civil suits, persons aggrieved for that. And normally, and it is also backed by the Justice Department, which actually criminally prosecutes some of these things. And that's -- I think our own litigation aside, the history of the Wire Tap Act as a privacy protector I think is actually not that bad because it sets a clear rule and it has clear compliance possibilities.

The only thing that I would add is I think that in this era where we do need to make sure that the kinds of private rights of action we create definitely include mass tort type actions, class-action type vehicles, because otherwise you are not going to be able to really

-- I would much rather rely on the efficiency of some sort of a private class litigation than of the political whims of whether or not a state attorney's general, et cetera, et cetera, get involved.

MS. RICH: Ellen, what do you think policymakers should do to encourage privacy-enhancing technologies? In the broad sense.

MS. BLACKLER: I wanted to go back to what someone over here said about objectives, that if we had a clear objective you can kind of work through with the people who build product, how to mean it, and kind of balance this need for creativity.

I think maybe some of what's happening is the objectives have shifted and they haven't been well articulated. So we -- the FTC is talking about notice doesn't seem right anymore. And so what is the new objective? I think we have been circling around this idea of transparency. People have talked about that today as different than disclosure. Telling me what you're going to do in a privacy policy is not particularly transparent, but having a customer see what's happening when it's happening. And if you said to the engineers, 'Find a way for consumers to see that,' maybe you would get some answers that we can't come up with today, some product solutions that we can't come up with today.

And I guess I would add to that list of objectives this usability notion because I think that's where some of the technologies have not -- it goes to the adoption issued to me. Some of these are not hard technological answers. What's hard is making them usable to customers. And if we put some focus on that, we might also see some innovation.

MS. RICH: Let me stay with you then in that you -- your industry took a hit on packet inspection, being the gateway -- being a gateway to consumers and so much information. Is there a special role that you and others like your company can play in providing these protections through technology, because of the gateway rule that you play.

MS. BLACKLER: Well, we try not to use that gateway word. But since you have said it, I think we have looked closely at the market opportunity here. And one of the things that has come clear to us actually is that there’s -- for some reasons I mentioned earlier. There is actually not really so much that a network provider can do that fixes the solution, because there are so many ways the consumers can get at these products.

And I think someone mentioned earlier -- or I guess it was Alissa who said earlier you have an apps store, for instance, and maybe the applications on the apps store have been vetted and live up to some standard. The consumer can go to the Internet and have this exact same kind of capabilities happen with a whole different set of protections.

So it's really not as simple as finding kind of this silver bullet in the network, particularly when you keep in mind the consumers don't all want one thing. So where we've kind of started to coalesce is around is really this individual-control notion. And the opportunity for us as a gateway provider, really exists for other gateway providers. And it is really your trust relationship with the customer because they're paying you, they have high expectations of you, you're setting up service for them, and so that's an opportunity to educate them and maybe get their privacy preferences that you can then, on their behalf, help them work through their Internet experience. But that is probably the same for any a device owner, for a platform owner; anyone with that kind of direct customer relationship, I think, has the opportunity.

And it kind of goes back to what David said when we talked earlier about competing on privacy. I think it is actually a lot more complex for the customer. And you're competing on trust, not really privacy. And I think the customers have a sense that privacy is part of their trust relationship, but it's really only one part.

MS. RICH: Speaking of David.

MR. HOFFMAN: Just struck listening here, as I've been listening and drinking my water and my bottle has been getting more and more empty, and so it seems like that's the theme of the panel, that the glass has gotten more empty.

(Laughter.)

MR. HOFFMAN: It seems like we're getting a dire message, things are horrible, we need a completely new construct. Peter just arms with me new ammunition, and now it's much more fuller, and I -- what I'm using -- I think we've built a foundation over the past few years that provides us with real opportunity moving forward.

I actually think -- you asked a question earlier that launched us into this. Well, reasonableness is too vague, but prescriptive, we don't want to do -- I think if we look at some of the Commission's Section 5 security cases I think we've got an excellent example there of cases where the Section 5 itself is a very high -- or a very amorphous standard. But then you've got people really coming together to define really what is unreasonable in this context.

I think another great example of where those kinds of messages are being sent, we're building the foundation, is the accountability work that is going on right now. I talked a little earlier about bringing the different institutions together, the regulators, the consumer advocates, the NGOs, and industry together. I think we're going to come up with, over the next couple years, a general concept of what an accountable organization looks like. And I don't think that accountable organization is going to be so prescriptive that, for my company that makes things and I need to have a process that is designed of getting to my engineer, might be a very different process than Ellen's company, that has a very different business model for what they do. But there is going to be similar themes within that that then would provide regulators the ability to be able to assess that and say is that entity running an accountable organization by that model.

I think we have got a lot of good building blocks to work from, I think there are a lot of good possibilities for us to go towards now.

MS. RICH: Well, and the Commission's data-security cases, even though we talk about them as reasonableness, it is the whole process from our safeguards rule, which is you do a risk assessment and then you design safeguards and then you evaluate risks in these particular areas and then you go back and you evaluate again to see if your systems are working, et cetera. So it is more specific than reasonableness.

At least in the data-security area, has that model actually spurred greater use of technology to protect data?

MR. HOFFMAN: Well, I would want to change your question. I think what I want to say is has it created more use of technology or has it increased better use of technology through the use of better business process. From what we see, we go out and interview all of our customers' customers, the chief information officers of the major company is out there, and the answer is clearly yes.

If you went back ten years and you asked what the processes were around information security and you looked at what they are now in these companies, it's lightyears ahead. And I think the FTC played a big role there.

MR. CULLEN: So just --

MS. RICH: That's a good way to be ending this panel.

(Laughter.)

MS. RICH: Well, Fred has his card up a long time. Can I go to him?

MR. CULLEN: Can I just close with -- just with one thing?

MS. RICH: Oh, but you've conspired to go? Okay.

MR. CULLEN: Yes. I mean David just kind of articulated what I'll call this tripod. In the business sense it's people process and technology. I know you have asked the question a lot of times about technology, but I think it is really important to say that technology is just one part of a solution.

If you think about it from the consumer angle, it's a combination of technology, education, and some form of regulation or government policy.

MS. RICH: Fred.

PROFESSOR CATE: I am just a little concerned that we not end by having totally abandoned the side of consumer privacy-enhancing technologies because I think we need to be clear about the failing so that we have a better understanding of if there is a role what that role might be.

I don't think anybody can prove there has not been a market failure here. But if you look at the available evidence what we know is that not merely are consumers not buying this stuff, they're not using it when it's given to them, so it doesn't look like a market failure.

In other words, when my browser says, 'Don't go to this Website, we think it's dangerous, and it turns the bar red at the top,' and we know because the researchers are in this room who do that research that people click right through those, we're not talking about the government mandating the technology, the government would have to mandate that I follow the technology or it would have to say Microsoft now has to ship Explorer that shuts down when I don't do what it says to do. It just seems like we really have a serious problem here on the consumer side of privacy-enhancing technologies.

So if they are going to play a role, and it's particularly not all together to clear to me that they are except as bundled, it's going to be a really tough road to hoe to get them in place, since we know that even when they're there we can't get people to use them. And I am not talking about complicated places like my firewall where I don't know what it means when it asks will I accept this communication on port 45, you know I know what it means when it says, 'We think this is a fake Website.'

The other sort of piece of this I guess I would just reflect on, I rarely, in fact I virtually never disagree with Lee, but I would not at least as a starting place look for mass tort litigation as a good place to start here trying to create incentives. Not because I don't think it can play any role at all, but because I think there are a lot of better places.

And you know it was frankly right here at Boalt Hall a year ago that we had the breach conference. And at that time I think it was 165 class action litigations on breach notices, not one of which had there been any damages found in. I have no idea whether there was harm or not, I'm not arguing that one way or the other. What we know is that there have been hundreds of million of dollars of attorneys' fees spent, if there had been harm, no individual had been compensated. And as much as I love attorneys, and I really do and I think they're fabulous, and I'm sorry that people have criticized them on this and other panels, but --

(Laughter.)

PROFESSOR CATE: -- I think it is a better place for the Commission and frankly other regulators to think about setting forth clear standards, leading processes that lead to clearer standards, identifying objectives rather than starting with let's let courts try to figure out on their own in kind of the mass tort litigation setting.

MS. RICH: Well, I really don't want to end on a court point, Lee, do you --

MR. TIEN: Well, I wanted to point out that I was not -- I did not mean to imply that that would be like the only thing. What I meant to say is that, and maybe even did say, was that this was simply one particular -- one thing that should not be automatically excluded from the pallet of tools. And because what we have had over the last several years has been quite a few instances of seeing that we just don't get enforcement from a whole variety of places where you might expect enforcement or you might expect to try to get liability.

If we really do agree that this is a problem, then we should try to practice sort of a multiple redundancy strategy in terms of how we are going to get to the optimum level of precaution in society rather than attempting to sort of hit the bullseye right now, which can take five, ten years, and then you are not sure you are going to get there anyway. I think there is something to be said for a little bit of organized chaos in this area.

MS. RICH: Well, I actually want to end on -- I have to end, but I want to end on the people, processes, and technology point because that's a refrain that we use at the Commission all the time too. And it's a good way to end this second roundtable because this roundtable is about technology, but it's really part of the larger whole of people, process, and technology in privacy.

So thanks to the panel. And we're going to have Chris Olsen come up for some brief closing remarks. Thank you very much.

(Applause.)

CLOSING REMARKS

ASSISTANT DIRECTOR OLSEN: Thank you to the last panel. I am going to make you all sit here for at least a few more minutes. I will be brief.

Before I provide a few remarks I must thank everyone who worked so hard to put this event together. Of course it would not take place without the assistance of Chris Hoofnagle, Robert Barr, David Grady, and Louise Lee at Berkeley, as well as the Berkeley law student volunteers: Liz Eraker, Vivian Kim, Colin Hector, Yan Fang, and Jenny Yelin.

Our own FTC staff has gone above and beyond the call of duty not just for this event but for several months putting together the series of roundtables: Loretta Garrison, Katie Harrington-McBride, Peder Magee, Michelle Rosenthal, Naomi Lefkovitz, Katie Ratté, Laura Berger, and Randy Fixman.

Today's discussions --

(Applause.)

ASSISTANT DIRECTOR OLSEN: Today's discussions were certainly illuminating. The first panel was chock-full of issues. We delved into the consumer privacy arms race. We learned that consumer efforts to block third-party cookies may be thwarted by Flash cookies or, even worse, supercookies.

We also heard about emerging developments like digital signage. We explored in more detail a topic raised at our first roundtable, whether personal data may truly be anonymized, and we examined the development of privacy-enhancing technologies and their role in protecting consumer privacy. This led to a lengthy discussion of genies and bottles. Who would have thought.

One point that came out of this panel is that technology alone may not be sufficient to protect consumer privacy interests and that they have to be -- they may need to be supplemented by policy solutions.

Our social-networking panel started with the discussion of the many benefits of social-networking services. It featured a healthy debate about consumer exceptions and the extent to which extensive sharing of personal information is well understood by consumers. Some said clearly yes, some said clearly no.

We spent a great deal of time examining third-party application issues. We heard the comment "data is the lifeblood of applications." We looked at the issue of who bears responsibility for the privacy and security practices of third-party apps. Is it the platform, is it government regulators.

Finally, we examined the portability issue and whether consumers can easily transport their online lives to another site. If portability is difficult, does that give platforms a freer hand to change the rules of their service without losing customers?

Our cloud computing panelists focused on enterprise uses of cloud and examined the privacy issues raised by the falling costs of data storage and the ease with which it may be maintained over time. Again we heard a quote similar to one we heard on the social-networking panel: "More data is always better than less, and we'll figure out what to do with it."

We also debated the wisdom of greater transparency for business practices in the cloud and noted the jurisdictional complexities that we have to keep in mind as we move forward.

Mobile computing focused us on two significant issues: The extent to which location-based services were proliferating really in an explosive way, but perhaps in an environment without consistently-applied rules or standards. And the degree to which transparency of information-sharing practices is happening successfully on mobile devices.

There was some agreement that some consistent principle should apply here but perhaps not consensus on what those principles should be.

And, finally, our last panel explored the intersection between technology and policy and Fred's love affair and hate affair with lawyers. Building on the discussion in the first panel, our last group of experts discussed ways in which our policy framework may create incentives to protect privacy interests and to build privacy protections into new products and services at the outset.

We heard from our international colleague about progress that the EU has made on this front and I am sure there are lessons for us there.

That brings us to an end for the day. Our examination of rapidly-developing technologies like social networking and cloud and mobile computing may call to mind at least for some what historian Lewis Mumford said about technology years ago, "Western society has accepted as unquestionable a technological imperative, not merely the duty to foster invention and constantly to create technological novelties but equally the duty to surrender to these novelties unconditionally, just because they are offered without respect to their human consequences."

Our expert panelists deserve our gratitude for helping us examine these technological issues and their human consequences. We look forward to equally robust and engaging discussions at our third and final roundtable in Washington on March 17th. We hope to see you all there and we thank you again for coming.

(Applause.)

(The Roundtable was adjourned at 6:06 p.m.)

CERTIFICATION OF REPORTER

PROJECT NUMBER: P095416

CASE TITLE: PRIVACY ROUNDTABLES

HEARING DATE: January 28, 2010

I HEREBY CERTIFY that the transcript contained herein is a full and accurate transcript of the digital audio recording transcribed by me on the above cause before the FEDERAL TRADE COMMISSION to the best of my knowledge and belief.

DATED: February 11, 2010

____

SUSAN PALMER

CERT 00124

CERTIFICATION OF PROOFREADER

I HEREBY CERTIFY that I proofread the transcript for accuracy in spelling, hyphenation, punctuation, and format.

____

NANCY PALMER

CERT 00121