FEDERAL TRADE COMMISSION

EXPLORING PRIVACY: AN FTC ROUNDTABLE DISCUSSION

Wednesday, March 17, 2010

8:30 a.m.

Federal Trade Commission

FTC Conference Center

601 New Jersey Avenue, N.W.

Washington, D.C.

FEDERAL TRADE COMMISSION

I N D E X

P R O C E E D I N G S

(8:30 a.m.)

WELCOMING REMARKS

MR. OLSEN: All right. If everyone will get settled, we're going to start now. I'd like to welcome everyone to the third and final roundtable in our series, Exploring Privacy. It's great to see that we've carried the momentum over from roundtable one through our Berkeley event and now to our final event here in D.C.

I need to make a few housekeeping announcements. The first, and perhaps most important to at least one individual, is we located an iPhone charging in a wall outlet, and it's available at the registration desk up front.

There are food and beverages available out in the hallway. There's also a list of other eateries available at the registration desk. Restrooms are located through the lobby. Don't go through the security stands. Go around past the elevators.

There's a Wi-Fi code for you to use to get broadband. The code is CABE 010808. There's also a brochure outside that has that code.

Anyone who goes out of the building without an FTC badge will have to come back through security. So, make sure you build in some time for that.

This is perhaps the most exciting announcement. In the case of an emergency, you'll have to evacuate the building and you'll go outside the building -- New Jersey Avenue is just in front. Across the street is Georgetown Law School. You go to the right front sidewalk at Georgetown Law School. We actually have a rallying point in case of an evacuation.

We'll have questions today. We'll have people in the audience with question cards. So, if you have a question during the event, please raise your hand. Someone will come to you with a question card. I think you have cards in your packages, as well. So, you can fill out a question and people will pick them up and deliver them to the moderators. For the web audience, we're also accepting questions. You can email them to privacyroundtable@FTC.gov. So, that takes care of the logistic announcements.

We're very pleased this morning to have Commissioner Pamela Jones Harbour provide opening remarks all the way from Barcelona. And we're very pleased that we worked the technology out, hopefully, so that this will be a seamless process. So, Commissioner Harbour, welcome.

INTRODUCTORY REMARKS: COMMISSIONER PAMELA JONES HARBOUR

COMMISSIONER HARBOUR: Hello. Welcome, Chris. Good morning. And welcome to the third FTC Exploring Privacy roundtable. Thank you very much, Chris, for your introduction. And let me personally thank all of the talented FTC staff who have worked tirelessly this past year to make these events happen.

You've heard where I am. Yes, I am in Barcelona, Spain, coming to you by video. A few hours ago, I delivered one of the keynote speeches to the Secure Cloud Alliance 2010 event. But I certainly did not want to pass up the opportunity to deliver remarks today at the third and final privacy roundtable.

And when I spoke back in December, I mentioned that I soon would be leaving the Commission. This time, I am really serious. I recently announced that I will depart on April 6th and this will be my final speech, albeit 3,500 miles away. And for the last time, I note that my remarks today are my own and not necessarily those of the Federal Trade Commission or any individual Commissioner.

I've said it many times before and I will say it again today. Protecting consumer privacy is of utmost importance. It must be a driving force for businesses in all stages of product and service development.

Unfortunately, many of the companies that consumers look to as leaders and that we expect to be leaders still have not taken this message entirely to heart.

First, I want to challenge what I see as a dangerous precedent being set by some of the biggest and most influential technology companies when they publicly expose consumer data. And, second, I want to challenge companies that are not adequately protecting consumers through SSL technology.

At the last roundtable in Berkeley, I discussed the comments of a technology executive who claimed that privacy expectations and norms are changing. More recently, since the Berkeley event, the press has recycled the comments of another prominent tech executive who stated, if you have something that you don’t want someone to know, maybe you shouldn’t be doing it in the first place.

Speaking for the last time as a regulator, let me be very clear. I could not disagree more with that assertion. Privacy is a fundamental right that people do care about. And I believe that the Commission and my fellow Commissioners would share this opinion. The Commission will continue to view privacy as an important value as reflected in the norms and expectations of consumers until it is proven that consumers feel

otherwise about their privacy.

The Commission will continue to evaluate consumers' preferences and armed with these insights, I hope and expect that the Commission will continue to shape the conversation about the intrinsic value of privacy. But make no mistake, the Commission will unfailingly step in to protect consumers where we believe the law has been violated and that includes violations relating to privacy promises.

And I'm going to be even more specific in my admonition to provide some concrete examples for today's discussion. The recent launch of Google Buzz was, quite frankly, irresponsible conduct by a company like Google. I would use that same word to describe the prior rollout of Facebook's new privacy settings as well as the November 2007 release of Facebook Beacon. But, for now, I will focus on the Buzz example.

Google is one of the greatest technology leaders of our time. Google consistently tells the public to just trust us and has adopted a company motto "do no evil." We have high expectations for Google as a corporate citizen. But for me, based on my observations, I do not believe that privacy, consumer privacy, played any significant role in the release of Buzz. In the rush, perhaps, to compete with Facebook, Foursquare,

Twitter, FriendFeed, Loopt and a host of other companies, it appears that Google did not think through the privacy implications of this launch.

New technology such as Buzz, like some of the updated features offered on Facebook, represent a laudable effort to help consumers integrate and make sense of the daily overload of information that bombards them via email, photos, blogs, tweets, news feeds and the like. And, today, consumers tend to have separate online accounts for a variety of services and often they maintain multiple profiles to separate their personal and professional uses. Plus, many companies do one thing very well, and accordingly, consumers are then willing to enter relationships with multiple firms.

A common characteristic of the most successful web 2.0 companies is that they thrive on the network effect. That is to say, the greater the number of users or number of inputs, the better the experience, which further enhances the trend toward interacting with multiple data sources.

When Buzz was launched, Google described its function as finding relevance in the noise. It is no wonder that seeking to capitalize on network effects, Google decided to build its service by turning to its installed base of approximately 150 million Gmail users.

Unfortunately, to my knowledge, none of those users were consulted before Google unilaterally decided how best to use their data. When users created Gmail accounts, they signed up for email services. That is their primary use of Gmail.

Several years ago when Google first introduced Talk, many users were taken aback that their email address book contacts were automatically suggested as Talk contacts. Publicly, there was a backlash and Google rolled back the Talk offerings. But the company apparently failed to learn from that prior mistake. Buzz was designed as a social network for users, but the net was cast too widely. News reports indicate that the company claims to have tested Buzz extensively with thousands of employees. The problem is Google employees are, in no way, representative of the Gmail user base, a combination of young, old, tech savvy, novice and so on. The Buzz product business manager admitted as much, saying that getting feedback from 20,000 Googlers does not equal Gmail users in the wild.

So, think about it. When Gmail first emerged, social networking was barely even a reality. When consumers, especially early adopters, created their Gmail accounts, their expectations did not include social networking. In my view, therefore, a reasonable consumer

would consider the initial opt-in of Buzz to be a material change in her relationship with Google. Consumers, not companies, should exercise the ultimate decision on whether they want to sign up for new features that might expose additional data.

I am especially concerned that technology companies are learning harmful lessons from each other's attempts to push the privacy envelope. Of course, providing new features to users and making the user experience more enjoyable are excellent goals. These efforts may win new users while also building additional loyalty in the existing user base. But even the most respected and popular online companies, the ones who claim to respect privacy, continue to launch products where their guiding privacy principle appears to be throw it up against the wall and see about if it sticks. And if not, we can always pull it back. Deeds speak louder than words. And this is turning into a dangerous game of copycat behavior.

And unlike a lot of tech products, consumer privacy cannot be run in Beta. Once data is shared, control is lost forever. In the extreme, it is only a matter of time before one might imagine the introduction of new features that incorporate, for instance, genomic information or data from public health records. The

privacy stakes will only get higher. And I realize that perhaps companies continue to take a testing the water approach to privacy because no regulatory agency has sent a clear message that this behavior is unacceptable.

In my opinion, that message may need to change and I would like to see the Commission take the position of intolerance towards companies that push the privacy envelope, then backtrack and modify their offerings after facing consumer and regulator backlash. In the meantime, however, companies should exercise greater responsibility and be more circumspect before launching game-changing products.

Computer algorithms should not be trusted to interpret consumer's privacy expectations. Consumers still have an expectation of privacy. These norms do not change and cannot be assumed away every time a company wants to compete in a new market. We cannot accept a new paradigm where products and services do not offer user choice, materially changing the bargain consumers understood when they first established the relationship.

Now, I don't want to be accused of harping only on Google. So, let me turn to my second admonition, which is targeted at a large number of prominent firms and which addresses an important issue of data security. I worry that many consumer-facing computing services have

significant data security vulnerabilities, especially services offered in what we call the cloud.

Encryption technology is already built into every popular web browser, but here is an unpleasant truth. Many popular services employ encryption technology and only transmit initial log-in information such as user names and passwords. All subsequent data is sent in the clear, unencrypted. This problem affects services such as Microsoft Hotmail, Yahoo! Mail, Flickr, Facebook and MySpace. This practice exposes consumers to significant risks when they connect to popular cloud-based services using public wireless networks in coffee shops, airports and other public hot spots. Without encryption, user data is easily intercepted using freely available, off-the-rack hacking tools.

And I spoke last fall at the International Conference of Data and Privacy Protection Commissioners in Madrid, and one of the most memorable speakers was a white hat, or ethical hacker for those who aren’t familiar with the term. And during his presentation this hacker -- ethical hacker demonstrated how he easily could break in to a network computer in a matter of mere minutes. It was very sobering indeed.

Many users of cloud computing services lack the basic security protections that users of traditional PC-

based software often take for granted. These vulnerabilities are easily preventable. Many web-based services, including online banking and certain online merchants, operate securely over wireless networks.

As a notable example, many banks in the financial sector use the industry standard secure socket layer, SSL, encryption protocol to protect their customers' information. These encryption technologies are widely available, yet many service providers choose not to implement these technologies for all data transfers and instead continue to provide products and services with unsafe default settings. Even though these service providers know about the vulnerabilities and the ease with which they can be exploited, the firms continue to send private customer information over unsecured Internet connections that easily could have been secured.

And so, my bottom line is simple. Security needs to be a default in the cloud. Today, I challenge all of the companies that are not yet using SSL by default -- that includes all email providers, all social networking sites, and any website that transmits consumer data -- step up and protect consumers. Don't do it just some of the time. Make your websites secure by default.

Let me end by saying that I've been speaking

publicly and have been very outspoken on privacy and data security issues for six and a half years now. And I have continually pushed companies to be leaders on privacy and data security. And I hope my words have resonated with some of you and that commentators and industry representatives will thoughtfully address my concerns. And now that I am leaving the Commission, the voices of two new Commissioners will emerge, Edith Ramirez and Julie Brill, are both incredibly bright and talented. And I know they will continue to fight on behalf of consumers as I have tried to do all of these years.

Let me end by saying it has been my great privilege and pleasure to serve the American public. Thank you.

(Applause)

MR. OLSEN: Thank you very much, Commissioner Harbour. Now I'd like to welcome Bureau Director David Vladeck for opening remarks.

SETTING THE STAGE: DAVID VLADECK

MR. VLADECK: Good morning. Let me start out with some thank yous. First of all, thank you all for coming. We are now down to the hardcore, but it's great to see that there's such a good turnout today.

Next, I really would like to thank Commissioner Harbour, not just for her thoughtful remarks this morning, but for her stalwart leadership within the Commission on privacy matters. We will miss Commissioner Harbour, but we know that her departure from the Federal Trade Commission will not steal her voice on privacy matters.

I also want to thank our panelists today for sharing their formidable expertise. These roundtables have been greatly enriched by the participation of panelists like the ones today and we are very grateful for their participation.

Before we get started today, I'd like to highlight four themes that have come up time and time again in the roundtables and end by explaining where we're going with all of this. First, we've discussed extensively the benefits and risks of technology in the privacy context. It's hard to believe that the Netscape browser revolutionized the Internet, opening the way for commercial uses of it just 15 years ago.

Since then, geometric increases in the computational capacity and data transmission speeds and cheaper and cheaper storage of data have had huge implications. These steady innovations have created benefits to consumers thanks in large measure to the flow of information that it makes possible. But these advances have also created new risks for consumers.

A few years ago, Tim Berners-Lee cautioned that IT professionals must keep in mind that -- and now I'm quoting -- "Data is a precious thing and will last longer than the systems themselves." Well, when data hangs around, odds are it will be useful for some purpose that may not have even been envisioned when the data was collected, and that presents challenges.

In addition, the march of technology has blurred and indeed threatens to obliterate the distinction between PII and non-personal information, especially given the shear volume of information that is now collected about individuals.

Catherine Deneuve, who I've always admired, once spoke for all of us when she quipped, "I like being famous when it's convenient for me and completely anonymous when it is not." On the web, at least, it is getting harder and harder for individuals to choose anonymity. And technology has enabled companies to

surveil people to an unprecedented degree, both online and increasingly offline.

Second, we have discussed privacy challenges raised by emerging business models. Business models have changed as quickly as the technology, creating new markets overnight. What did consumers know about cloud computing or even social networking as recently as five years ago? The continual emergence of these new models, too, means that consumers are often presented with unfamiliar or confusing situations where the nature of the commercial bargain, in terms of privacy, may not be clear and may be constantly shifting.

Not surprisingly, consumers understand little about how their information is handled, whether by companies they share with directly or by companies that work behind the scenes like data brokers, ad networks and application providers.

Third, although new technologies and business models have raised privacy concerns, they have also been used to innovate to protect privacy. For example, several companies have introduced tools that consumers may use to access the Internet categories they've been placed in and to change how they've been categorized. And non-profit thinktanks, the future of privacy forum, together with marketing communications company WPP has

led an effort to develop and test an icon that would alert consumers how to get more information and how to make choices about how their information is being used for behavioral advertising. This is all to the good.

Fourth and finally, there's been little satisfaction with the privacy approaches that have been pursued to date. Privacy policies are not located where consumers can find them. They're too complicated, they're too vague and too long for consumers to really understand them. While there's widespread agreement that the information processes we use should be transparent, we're still exploring effective ways to disclose what information is being collected and to give consumers a meaningful opportunity to control its use. And, of course, we all know that once information has been shared, there's no way to get the genie back into the bottle.

Although we've covered a lot of ground in the first two roundtables, we've left some big questions for today. Our first panel tackles one of the big questions of the Internet. Can we build security and privacy into the Internet after the fact? That is, can we create a secure authenticated structure on top of a foundation that was built to be trusting and open?

Next, we'll tackle health privacy issues,

examining another great puzzle. How do we reconcile individual interest in privacy, particularly about health issues, with society's interest in getting research, epidemiologists and others the information they need to improve our collective health?

Then we'll address the question about sensitive information more broadly. Is there a consensus that particular categories of information are sensitive and deserve heightened protection, or is information about certain kinds of people so sensitive that they should be treated with special care? For instance, information about children. Or is sensitivity simply in the eye of the beholder? Are there policy approaches that would enable people to apply their preferences themselves without the need for some kind of consensus?

The final panel will wrap up with a discussion about what we've learned and where we go from here. I expect we'll hear a lot of the same themes and questions come up. How do we make information practices transparent to consumers and how do we give consumers appropriate tools to make their preferences known? Also, how do we create incentives for companies to consider privacy before rolling out new business models or new service models?

Many people have asked me, where do we go from

here? Once this roundtable is concluded, what are the FTC's next steps? Well, I think, to be candid, we're not certain. The first thing we're going to do is we're going to sit back and we're going to digest everything we've heard. We've made detailed records of the first two panels. We'll do the same with this. We'll need to go back and study them. We will put together our thoughts and recommendations, if any, and we will make those public.

We will then solicit your input. We want to be as open and transparent as we can and we will need your helps and your thoughts. So, we will have a very public process on this. We've had great, great assistance as we go forward. We look forward to more of that in the future.

Before we conclude, I want to say one final word of thanks this time to the staff that has worked for months to make these roundtables happen. It's really hard to explain just how much time and effort goes into putting these panels together and to doing the research that is discussed at these panels. No one would have ever thought that a President from Chicago would shut down the government because of a little snow. But during DC's recent "Snowpocalypse," the entire city was shut down for more than a week. But the roundtable team did

not miss a beat. They worked tirelessly through the storm. We're not like the Postal Service. A little snow, sleet, rain or four feet of snow is not going to stop the FTC. They worked throughout that stretch to put this roundtable together. I greatly appreciate the dedication and care they've shown throughout in making these roundtables a success. So, thank you all very much and thank you for coming.

(Applause)

MR. OLSEN: Thank you, David. We're going to take a very brief break. I'll ask the panelists for panel one to come up and take your seats. We'll start promptly at 9:15. So, if you want to take a couple of minutes while Panel 1 gets settled, and then 9:15, we'll begin. Thank you.

PANEL 1: INTERNET ARCHITECTURE AND PRIVACY

MS. GARRISON: Good morning and welcome, everyone. I'm Loretta Garrison and this is my co-moderator, Naomi Lefkowitz, and we're going to moderate the first panel for the final roundtable this morning.

We're going to open today's final roundtable by stepping back and taking a hard look at the architecture of the Internet. We want to present a challenge to all of those technical folks in the audience and those of you who are listening in. And to our distinguished panelists who have come prepared today with all the answers to the questions we're going to ask them.

The panelists today, we're very delighted to introduce to you, are John Clippinger, this is to my immediate left and we're going all the way down the table. He's the co-director of the Law Lab at Harvard University Berkman Center for Internet & Society.

Next to him is Jules Cohen, director of Trustworthy Computing for Microsoft.

Then Peter Eckersley, who's come all the way in from California. He's a senior staff technologist with the Electronic Frontier Foundation.

Next to Peter is Ed Felten, who's the director for the Center for Information Technology Policy at Princeton University.

Next to Ed is Lucy Lynch, director of Trust and Identity Initiatives from the Internet Society.

And then we have Drummond Reed, who's the executive director from the Information Card Foundation.

And last, but definitely not least, Ari Schwartz, who's the vice president and chief operating officer for the Center for Democracy and Technology.

I'd like to remind audience members that you can submit questions to the panel by filling out a question card and handing it to FTC staff that will be walking around the room. For those of you watching this panel via the webcast, you can submit your questions by emailing them to privacyroundtable, that's all one word, at FTC.gov.

And to our panelists, if you want to speak at any time, please turn your name tent on end and wait to be recognized.

As you know, when the Internet was initially created, it was technically designed to facilitate communications among a number of researchers at various universities around the country and what is now known as DARPA, the Defense Advanced Research Projects Agency. This was a small, known, trusted environment designed strictly to share information as the participants worked on common projects. Since then, we've built on top of

that architecture a complex commercial enterprise, a social networking system, search functionality, none of which was contemplated or even envisioned at the time of the original design.

The challenge today to our panelists is to engage in a thought experiment and examine and discuss how you would construct an Internet today to accommodate these various enterprises and what change from that design we can apply to the existing architecture short of blowing up the Internet.

So, Peter, if you can start us off. If you could start afresh, how would you design the architecture of the Internet to design all of these activities to address the privacy and security concerns that we've heard throughout these roundtable discussions?

MR. ECKERSLEY: So, I can't necessarily give you a single answer to that question, but, you know, here's the new design, let's just go with this instead of the current Internet. But I can say that if you want to understand the privacy problems we're having on the Internet today, it's helpful to imagine taking a time machine back to the early '90s and looking at where today's Internet came from.

And what you would find is that there are a lot of the problems that we're looking at that were

essentially side effects or inadvertent design decisions that were made back in the ‘90s with the intention of just making the web work and making it work better. We could look at TCPIP, which is the basic protocol that most Internet software uses to communicate, and it has this property that the other side can always see the address that you’re using to communicate.

And then you can look at the web, which is a simple client server protocol, and say, so a web server always sees the addresses of the people who are reading each document. And these sort of things seem inevitable, but perhaps they weren’t inevitable, because if you look at the web, at the same time people are also using other protocols like email even and Usenet, where you couldn’t necessarily see the other person’s address whenever they communicated with you. In fact, back in the ‘90s, often there was a separation where some sort of federation of machines was talking to each other and you never got a message with the other person’s address traveling the whole way through the chain of communication. And there were special protocols, like Finger and iDent, that were used to separate policy with respect to privacy from policy with respect to communication.

And so, I think one way that we could think about re-architecting the web, if we could do things over

-- we can't necessarily do that now easily -- would be to say, well, does a web server need to see the user's IP address every time they connect and can we find a different model for that?

There are a bunch of other decisions that were made later in the '90s the way that cookies and Javascript and other things were added to web browsers that also have serious privacy consequences, and I'm sure other panelists will talk about some of those.

MS. GARRISON: John?

MR. CLIPPINGER: I think Vint Cerf was asked that question. He said, if you had a chance to do it over again, what would you do? And he said, it was missing an authentication layer. And by that -- and this is something that we've been very interested in is, okay, how do you know who you're dealing with and how do you start to develop -- I think we're going to have to think about -- I don't think about blowing up and starting new, but how did you build a new layer or how do you build something on top that allows you to have a principled way of knowing who you're dealing with and having -- sort of creating a kind of consequence for behavior at how people treat and disclose information?

I think what we've been talking about here with the traditional privacy format has been, how do you

sequester information? I think the issue is going to be how you control it and who has access to it and how do you enforce certain contracts or conventions of access through information. You can't sequester it. That point was made earlier. Personal identifying information can be constructed from non-identifying information.

I think there's a need to create a new kind of governance regime, a new kind of -- you have to approach it in a systemic way, not just in a piecemeal way. And my view is that it's very important -- the locus control really has to be on the user. You have to have a user-centric, interoperable system that allows people to control information about themselves and have a chain of trust that can be traced back to the individual. It's not to say that people are going to make all those decisions, but architecturally, I think that's a critical consideration.

So, going forward, I think we have to think about not just little piecemeal type fixes, but a very systemic way of thinking about it that uses a variety of methods all the way from new kind of encryption technologies to contracts to what kind of business models are used, what are the incentives, what kind of incentives to different companies and players and identity providers have that are aligned and can take a

race to the top rather than a race to the bottom.

So, my admonition is that we're moving from a technology to a social area. And in doing that, we're making very profound decisions about how people are going to participate and be protected in our society. So, we're building new kinds of institutions that have far-reaching implications.

MS. GARRISON: Well, one of the critical aspects of any redesign is going to be the usability and, in a sense, the invisibility of the change to the consumer. We're going to talk a lot about this later on, but certainly one of the ideas behind looking at the basic architecture is whether or not something technically can be built in or designed that would change the default so that it would make it easier for consumers to understand what's going on and to make informed decisions.

MR. CLIPPINGER: I couldn't agree more. I think that one of the things that we're looking at experimenting with is how people can see their information being used, who sees whom, who sees what. And you might have red, yellow, green information and when green information goes red, what causes that? A piece of information is somewhere where it shouldn't be. So, I'm here, what am I doing here? Have audit trails.

I think we have to move away from sort of complex, inscrutable legal agreements to where people can have an intuitive understanding. The expectation of privacy has to be reflected in the experience and certain norms that are adopted and relied upon. And this is new territory. But you're starting to see some very interesting designs.

But on top of that, I think you have to have the audit mechanisms. You have to have some kind of independent party holding others accountable for that. We'll talk about that later.

MS. GARRISON: Okay. Ed, did you have a comment?

MR. FELTEN: Sure Certainly, it's important to give users some kind of visibility and control over their information, where it goes, how it's used, and so on. But this is much harder to do in practice than you might expect. Today, users in principle have a certain amount of control over things like the privacy settings in their browsers. But, in practice, they really don't. Because the mechanisms that are used either involve asking the user millions of questions in pop-up boxes that the users quickly learn to click away, or some kind of very detailed browser privacy preferences, dialogue that hardly any users even open, let alone understand.

The real challenge is how to let ordinary users have effective control and real autonomy in this area without having to invest a huge amount of effort or learn a lot about how the technology works. And I think that requires some -- that's going to require some really clever advances in the basic models of user interaction online.

I don't think we can add this on with patches. I think we really need to think how does the user interact with the technology on a minute-to-minute basis and we need to build the technology where the user is revealing to the technology through the things they already want to do, what they want.

MS. GARRISON: Lucy?

MS. LYNCH: I want to drop back just a little to the question about actually re-architecting the Internet and about whether or not you need to blow it up to change it. There are two different conversations going on here. There's a conversation about the Internet, the entire Internet, the network, that communicates, and there's a conversation here about the web, which is most end users' experience and what happens above that layer.

And referencing John's comment, authentication needs to be built in actually at that network layer.

Users aren't the only ones who communicate on the network. Entities communicate. Machines communicate to one another. And it's essential that they be able to continue to communicate and to identify end nodes. The benefits of the Internet come from the distributed, decentralized hierarchical model that allows any entity to communicate with another one. You don't want to break that.

There are technologies being designed, and some of them are privacy aware like GeoPriv, that are built in at the network layer and you need always to think in a distinction, above and below the web, when you're talking about this. There are privacy concerns below the web, as well.

MS. GARRISON: Drummond?

MR. REED: I wanted to find an example of how you can achieve privacy by design, but also how hard it is. Again, I'm here as executive director of the Information Card Foundation. I want to point to information cards as a technology that has -- is about six or seven years' worth of work in its development to try to address, Loretta, exactly what you brought up, which is the usability of privacy.

A good part of what we're doing right now is educating audiences about if you want to give end users a

very easy way to authenticate to websites, to share information about themselves or from third parties about themselves, while also at the same time protecting their privacy, it's a difficult job.

I'll give a very specific example. With information cards, as an authentication technology, it's a way to sign into websites, the end user experience is simply one of picking a card out of a wallet. There's no typing of usernames or passwords. And, yet, the underlying technology will automatically -- you can pick one card and use it to sign into a hundred different websites. The underlying software will give a different private personal identifier to each of those 100 websites. They will not be able to correlate the information, the log-in experience. That's because it's carefully designed to do that.

The user doesn't have to understand anything about that. It's a simpler experience than log-in today. But the technology has been designed to ensure that no correlatable identifier is being shared across all those sites. That's an example of the kind of approach that you have to take if you're going to address what John talked about, privacy at this relationship layer that, I believe, is evolving and that we're going to need to address this issue.

MS. GARRISON: Jules?

MR. COHEN: I wanted to echo a couple points that have been made. It's not just about sort of some of the privacy questions. I think that it's worth up-leveling to this interesting question of, with respect to the hardware that I'm using on the Internet, the software that runs on top of that hardware and the people that use these other two things, how do I make trust decisions? And those trust decisions are broader than privacy. Should I trust this piece of hardware? Where does it come from? Should I trust this operation system, this application? Where do they come from? Who are the people behind them? And then should I trust the people that are using them?

Sometimes those are privacy decisions about where the data that flows through the system are and sometimes it's security decisions. And what tools does the user have to actually make those trust decisions and what information do they have on hand and what cues in the user experience are they provided with are some of the hard questions that we're grappling with.

MS. GARRISON: I wanted to ask all of you about some of the basic premises on which the Internet was developed or the web. You have a system of networks, it's peering, which is -- in a sense, in my mind, it's

related to the federal highway system, the super highways, then you've got the state roads, then you've got the county roads, then you've got private roads. Each of these can be built either in an organized way, or in a private sense if two companies want to share information, they can simply create that network or that connection and do it.

Does this basic autonomy of the Internet design actually create barriers or difficulties to addressing -- in a structural way, to addressing the privacy and security issues that we have? Peter?

MR. ECKERSLEY: I want to say no, actually. I don't think there's a problem with peering and the way that the Internet is a whole of little networks that are stitched together in a patchwork quilt. I think that works pretty well and I think if the protocols that those networks are talking to each other solve your privacy problems, at some layer, then that's going to work well.

I think the dynamic that is problematic is one where no one really owns the whole privacy problem. In the example I told before where the web creates this privacy problem by showing the reader's address to the server every time -- and it didn't have to be that way, email didn't have that property -- that was like a low level consequence of one protocol and it was a privacy

problem that wasn't solved there and the privacy problem got kind of kicked upstairs. Someone said, hey, we won't deal with this in HTTP, but if people want to solve this privacy problem, then they can go and invent a separate proxy protocol to hide their IP addresses.

And the problem is that when you kick these things upstairs, suddenly only 10 percent or 5 percent or 1 percent or less of people actually get the solution. So, I think the problem isn't with the way that the networks are stitched together, it's with making sure that someone is designing privacy and they're answerable to the users ultimately when they say, hey, why was I tracked by this person? You know, you need one kind of place that you can go to and say, fix this protocol until I get the privacy properties that I need from it.

MS. GARRISON: Ari, I saw you nodding your head. Did you have a comment?

MR. SCHWARTZ: I strongly agree with what Peter just said. I think there's a tendency to be concerned with how information is passed back and forth across the Internet because of the way that some of the original design went in, and also, because of the way that some network operators have been talking about discriminating against certain kinds of content. If we didn't have this discussion about going in and looking into the content of

the packets, then we would have less concern about that information being passed.

If we can build a more secure system that respects privacy in the protocols itself, then those concerns are addressed. And it has nothing to do with the -- you have lots of worry of the discrimination of packets. As long as we keep that basic end-to-end principle, we shouldn't have a problem of the structure of different kinds of entities and different kinds of peering agreements.

MS. GARRISON: John?

MR. CLIPPINGER: One caution I would say, I think one has to look at the emerging business environment and that where information is going to create value. So, there are going to be business models based upon aggregating information and making it available. It's sort of the next generation of Google. So, there are going to be very strong forces in the market to test the limits of those protocols and to reinterpret. And so, I think it's very important not only to have sort of the correct business incentives, but have the correct audit mechanisms because we're really talking at another level that's never existed before.

And recognizing that there's great wealth and opportunity and things that could happen when you use

this information effectively and you can inflict disease and a whole number of things can be done, so you don't want to sequester it. But at the same time, you want to have a set of rules, rules of the road, that are governance principles that are enforced quickly, transparently and effectively, and also, grow with the technology. Otherwise, it will get co-opted.

MS. GARRISON: Okay. I want to turn to the IP address protocol because, as you've discussed, an addressing system is fundamental to sending data packets over the Internet. Drummond, are there technical limits to masking this information to avoid tracking or are there other ways to address the tracking issue?

MR. REED: It's a very complex question. Another hat that I wear is I'm co-chair of a technical committee at an Internet standards body called OASIS and that technical committee is called XRI. It's for a new type of identifier for the Internet. And an easy way to explain where that fits is that if the plumbing layer that we're talking about between the hardware is using IP addresses to communicate and this next layer of the web is using URLs, you're connecting between browsers and servers for pages, the XRIs are designed for this relationship layer. XRIs are really designed to identify people, organizations, concepts, and to have

communications directly at that layer.

Imagine that you can actually have a messaging relationship where you're not communicating necessarily between IP addresses or between email addresses, but person-to-person and the communication is actually able to route itself to the right device depending am I trying to send John a short message about I'm five minutes late for this meeting or am I trying to send Ari a PDF file for something. It's a matter of being intelligent about the choice. That kind of communications routing and the associated rules, for instance, the privacy or security that can be applied to the message. That's the kind of thing that that layer can address. It's one approach.

I believe there are issues that transition from IPV 4 to IPV 6 has introduced both new capabilities and new vulnerabilities at the layer of IP addressing. URLs have their own set of issues. We're trying to address some of those at the XRI layer. It's one way that we can help address those things.

MS. GARRISON: Yeah, the IPV 6 issue, we had discussed among us, and although there had been some doubt that this would create any issues with IP addresses being collected and linked to information, there was a recent article about a company, Clear Site Interactive, which has acquired something like 100 million IP

addresses and of those were actually able to link email address, postal addresses, names and other registration information to actual individuals and they're going to initiate targeting based on that.

And, of course, with IPV 6, you're going to have static IP addresses increasingly assigned to individual PDAs, so you will have this direct linkage. This is actually exacerbating the problem of linking all of these bits of data, this sticky data, to individuals.

John or Peter, Drummond, any of you want to take that up? Drummond?

MR. REED: Lucy?

MS. GARRISON: Or Lucy, okay.

MS. LYNCH: I think there are a number of problems involved in that convergence that you're talking about, and it's exacerbated actually by introducing identity management technologies because there's a set of passive data that's collected that are the system identifiers, that give you one profile. But as people volunteer personal information in conjunction with that data, that's where that identifiability comes.

Because with a few exceptions like who is data, which is directly tied to the ownership of an IP address, the way they're building that conjunction is by taking volunteered data and system data and conjoining them.

That is not a problem with the design of the network. That's a problem with understanding what data you volunteer and how it gets used in conjunction with the other data that's available. So, there's a user education issue there and there's a compliance issue there. You need to gain consent in order to use that data --

MS. GARRISON: But, Lucy, if you go back to the earlier point that the IP addresses were not necessarily intended to be identified, but now they are and now they're linked, is that also not a structural problem, a design problem, as well?

MS. LYNCH: No.

MS. GARRISON: Okay.

MS. LYNCH: No. Users want service. You need to be able to deliver to their end node. Trust me, users want service. Whether or not they should be exposed because they get service is not the problem. But you need that identifier in order to deliver service.

MS. GARRISON: Ed?

MR. FELTEN: Sure. Talking about IP addresses as a way of tracking or linking, activity really, I think, puts the focus on part of the problem around tracking and linking, which is that there are so many different technological ways that sites or different

parties can track or link what people are doing. If I, as a user, want to avoid being tracked or linked, I need to have a strategy for dealing with all of those different tracking methods.

There's a very large perimeter that I have to defend technologically to maintain my anonymity when I want to. And if we're going to make progress to give users more control, we have to reduce the size of that perimeter, either through technical or other means.

MS. GARRISON: Peter?

MR. ECKERSLEY: Look, I think that's absolutely correct. I mean, I was going to make a point just about IPV 6, which is -- this is an interesting story. If you compare IPV 6 to IPV 4, we use IPV 4 today, but people are hoping that one day the Internet will use IPV 6 --

MS. LYNCH: I use IPV 6.

MR. ECKERSLEY: And a few people do. But there's a bit of a switching problem because you don't get much from using IPV 6 until almost everyone uses it. So, it's this hard bump for the Internet to get over. If you look at IPV 6, if everyone implemented it naively, it would be a privacy disaster in the sense that the specs tend to publish your Mac address in public view to the whole wide world. So, in fact, there's almost nothing you can do by default to avoid being instantly identified

as soon as you get onto the Internet. And so, that's kind of a bad thing.

But then the number of addresses that you get from IPV 6 has a much larger space than the mere 4 billion addresses in the current Internet. Those addresses, perhaps if we shuffled them the right way, that would actually give us the opportunity to make IP addresses less trackable because you could give people a new one every single time they popped onto the network and then you wouldn't have a problem with tracking by IP address.

Now, some people would say, oh, that's not good because it means that people can't run their own little servers on their own machines that have a persistent address for those and maybe that's a problem that we can solve by some other intermediate ways. There's a way to look up an address for a transient server and get the different shuffled IP address every time it changes. So, I think there are these consequences that come from these technical protocols, but Ed's point still stands, that if we want to talk about privacy, we need to not talk about just one of these things. We need to deal with this bewildering mass of different tracking mechanisms all at once, unfortunately.

MS. GARRISON: Jules, I want to turn to you

because when we had a discussion before, you said that in the work you're doing, as you build new applications for the web, you look at the user experience offline in order to design for online. But I want to look at the addressing issue and the sending of information. In a very over simplistic way, if I mail a letter to you, the post office delivers it, they don't record that I sent it to you on a certain date and they don't open it and read it. So, that's an offline experience. But, certainly, that's not the case online.

Do you have any thoughts about that or want to talk a little bit about the way in which you are mapping online -- or offline to online?

MR. COHEN: The context in which I think that it's really helpful to think about the relationship between the online world and the offline world is more in the identity management space. I'd be happy to talk a little bit about that now.

So, just for a little bit of context, I think we've figured out a lot of the identity management problems in the offline world reasonably well. We have methods that have grown up over generations, decades to figure out in a particular context if you want to prove who you are at a given level of assurance, you can do so. You carry around a wallet, as Drummond said. It has

maybe a driver's license, maybe a student ID, ATM card, a Starbucks card, corporate ID, and they all provide different information about yourself and about who you are in the real world.

And depending on the context, you might choose, oh, I'm going to show my driver's license because I'm at TSA; oh, I'm going to show my student ID because I want a discount at a museum; oh, I want to use my ATM card to get cash; oh, I want to use my corporate ID because I want to opt in to some kind of a service. And they're all used in different ways to access different services in the real world. And that model works pretty well.

But on the Internet, as John was saying, we don't have that functioning interoperable identity layer. It doesn't exist. And as a result, we have what's essentially a rather Kluge (phonetic) method of using usernames and passwords and shared secrets. I think we all know sort of the challenges with those, with phishing and with identity theft and the like.

When the thing that you use to prove your identity is something that anybody can type in on any computer anywhere in the world, to access the kinds of rich information we've been talking about, and not just the kinds of information that have been discussed here, but also bank account information, health care

information, life and death information, the really, really hard stuff, there's a challenge there.

So, one of the questions is we know we have this working interoperable model that works at a reasonably high level of fidelity in the offline world and provides reasonably good privacy protections in a bunch of contexts. How do we take what we have in the real world and move it over into the online world? And one of the things I think that you figure is that in the offline world, in the real world, there are moments when trust is created. When I go to the DMV and show my utility bill and my Social Security card and related, there's this trust that's created over the counter there with a human. There's an in-person proofing moment. At that point in time, that trust is bound into a plastic card and they hand it to me and then I can go reuse that trust offline to get services.

The same thing happens when I register for school; the same thing happens when I become an employee; the same thing happens in a bunch of contexts. In those contexts, there is a relatively high bar that I cross offline and trust is created.

And one of the challenges that we have online is that there are no similar in-person proofing experiences. It's pretty hard to get that level of trust

to be created online because you don't have a human making a trust decision at the outset. So, one of the things I think we need to do, and we can talk about this more over the course of the panel, is figure out ways to reuse pieces of trust that exist offline in online contexts at a reasonably high level of security and figure out ways to use those to make good privacy decisions about what happens with the subsequent data.

MS. GARRISON: Ari?

MR. SCHWARTZ: Let Ed go first because he's going to make one of the two points I was going to make, but he's willing to empty out his wallet to do it, which I was not.

MS. GARRISON: Okay. Ed?

MR. FELTEN: Thanks. So, I think we need to be careful about the analogy to the real world plastic cards. Here are the plastic cards that were in my wallet right now. All of these people know who I am, they know my name and address, and they could trivially link back to my identity and link their records together. There's a library card, frequent flyer, my work ID, credit cards, driver's license. All these people know who I am. They can link my activities together. So, I don't have great privacy protection there, at least as a technical matter.

MR. SCHWARTZ: My point was exactly the same

one, which is I think we can do it better online than we do it offline. And we should -- that should be the goal. The goal shouldn't be to do it exactly the way we do it online. I think we can learn from the way that we do it offline to help to try and figure out kind of a process to go about doing identity online. But the goal should be, as Drummond was saying before, how can we de-link information to solve the problem that Ed was talking about? How do we build transparency enough that people can see what information is held about them and make changes to it if it's wrong and if it's something that's used to make decisions about them in the ordinary course of business? Those are things that you can do online that you can't do with systems that were designed in the world of file cabinets.

MS. GARRISON: Before we migrate clearly into identity management issues, can we wrap up with just a couple of issues related to -- going back to the architecture and whether there are some structural changes, whether they're big changes. I haven't heard any big changes, but maybe there's some small ones that we can consider, which still would be important.

Peter, you've talked about some which you call low-hanging fruit.

MR. ECKERSLEY: Absolutely. So, I think maybe

this is a terrible analogy, but if we're going to talk about low-hanging fruit, perhaps privacy is like we're trying to make a fruit salad and in order to be a tasty fruit salad, it's got to have everything.

There is low-hanging fruit. And one point I really want to emphasize is Commissioner Harbour's call for SSL encryption. I think that's a tremendous idea. It's really low-hanging fruit. It's a protocol that we have that's already developed, it's already widely in use. And, in fact, it actually addresses the question you were asking just before about, well, the post office doesn't open our mail. Using SSL prevents the network from opening your mail and it's a great idea. It protects against hacking. It protects against all sorts of privacy problems. Not all of them, but it's low-hanging fruit, let's get it and let's put it in our fruit salad.

There are harder things that I think we should try to do. Ed mentioned before the fact that browser user controls -- currently, you need to be an expert, frankly, in order to -- and very patient. Both an expert and very patient in order to get anywhere with the browser privacy controls.

A question I wanted to ask him was, could we do better with blacklists, with something like the Adblock

Plus model where you have a list of the bad things that you need to block? And that's socially constructed. It's an institution. We could crowd source it. We could have everyone sitting down and studying the web and saying, wait, here's a new tracking company that has no relationship with the people they're tracking, let's just block them. Could we do that? Would that be a feasible model? So, that's a harder fruit to get, but maybe we could get it.

And then maybe there are other really important ingredients that tie into the next subject we're going to talk about. And this is a question for all the identity management people. Can we get anywhere with identity management systems that give you throw away identities that are nonetheless trustworthy? I know that the cryptography is there. There are these fancy protocols called zero knowledge proofs that, in principle, allow you to be -- to show up at a website and say, hey, I'm not going to say who I am, but I can prove that I'm a person in good standing. Is this a solved problem? Are we close to solving this problem? It's not exactly my field, so, actually, I'd love to know the answer.

MS. GARRISON: Okay. For John, we have a question for you from the audience. You said earlier in our conversation that we're starting to see interesting

designs for giving consumers more control over their data flows. Can you briefly describe some of those?

MR. CLIPPINGER: Actually, this builds on an earlier point. With the notion of iCards, I mean, we were involved in developing something called Project Higgins and the analogy was to having different kinds of cards. But the difference is -- and I think we can do it better in the online world -- is that only the end user, the person knows that can link them and you can have a different card generate an identifier -- a femoral identifier.

I think we're going to move to a point where you're going to have authenticated anonymity and you need to separate -- this is my view -- separate out sort of the physical person from the virtual authenticated person. Because the real consequential damages are done to the individual and it has life consequences when the abuses happen. They take your DNA information.

But you also have a social contract in the sense that information is jointly created about you, you have medical treatment, you get FICO scores, things like that. So you can't disassociate. But there may be mechanisms that allow us to have the cake and eat it, too. And I think this is new ground. There's new thinking on this.

The zero knowledge proofs, I find fascinating and very promising. We had worked with Microsoft and a company called Credentica that they acquired and that technology is coming on board that I think can have an amazing impact.

MS. GARRISON: Ed?

MR. ECKERSLEY: This idea of authenticated anonymity is actually something that today's password system gives us, when it works, when we have secure passwords and so on. That is, I can set up a user account and password on one site, a different user account, different password on another site, and they're inherently unlinkable if I choose those well.

But the problem is that there are so many other ways that those sites can link together, the fact that, yes, this really is the same person. And once they have connected those dots, it doesn't matter how I authenticate myself to the site. Again, there's this perimeter you have to defend. Because if the link is made ever between my activities on the two sites, then there's no undoing that.

MS. GARRISON: Jules?

MR. COHEN: I just wanted to make a comment about the zero knowledge -- I'll make two comments. One is that we're on the cusp of a very sort of broad and

deep conversation on identity management, and we could do it right and we could do it in a way that doesn't exacerbate all the kinds of problems we're talking about. And the zero knowledge proofs are a way to do that to allow unlinkability -- to allow a number of properties, unlinkability, untraceability, a number of properties that can improve the situation, and at the very least, don't make it worse. But it certainly doesn't address the plumbing layer issues.

I would just note that we released last -- a couple weeks ago at RSA, we released the foundational pieces of the zero knowledge technology. It's called UProof, under the open specification promise. So, developers can go build on top of that freely, and we're hoping to see a significant uptake of the use of that technology.

MS. GARRISON: Okay. Drummond?

MR. REED: Before we leave the technology layer, I want to build on what Jules just said. If folks are not clear when this term is used, zero knowledge proof technology, I want to make it very clear. Imagine you have an information card that is able to prove -- that actually has your birth date on it, okay? If you share that information with a site, it actually doesn't take much more than your birth date and maybe your zip

code, one or two other pieces, even if you're not sharing a linkable identifier, they're able to correlate you or they're going to be able to link you. And this is just one example of the many ways that can be done.

With zero knowledge proof technology, that information can be there and when it's shared with a site, technologically, the site can prove that you are over a certain age but not get your birth date, okay? And it is a significant step forward. It's been widely vetted. Microsoft's acquisition of Credentica and now their release of UProof at RSA, I think, is a major step forward. Information cards were designed to carry any type of token, including these new UProof tokens. So, this is something we hope to see coming into use fairly quickly now. It's been theoretical for quite a while, but now it's a real thing and what it could mean for privacy or authenticated anonymity, as John puts it is, I think, significant.

I want to say one other thing on the technology layer before we move up. The other thing that I think is happening -- and I'm putting on another hat, which is the XDI technical committee at OASIS. XDI has a protocol based on XRIs and one of the key things it does is bind data and policy. It is a way of whenever you share information, if you're able, on the part of the person

sharing the information, to say this is the policy bound with it, this is the terms under which I'm sharing the data. In XDI, we call that -- it's the concept of a link contract. If you're able to do that, it introduces a new paradigm for how that information, that data and its use can be respected throughout that life cycle, throughout that chain of trust, as John was talking about it.

Now, actually observing those policies is not something necessarily technology can enforce, but doing the binding and having a cryptographic way that that binding can be observed is something that technology can do. So, it's sort of how the two pieces can work together.

MS. GARRISON: Well, we want to talk a little bit more about the technology and policy together and also bring in enforcement. We'll do that after we do more discussion on identity management.

But there's a question that's also come from the audience. Peter, I think this is to you. Isn't the focus on SSL and the allegedly new problem of in the clear traffic to the cloud really an old problem? How is this any different from truly ancient email transport protocols like SMTP or POP that involve similarly unencrypted traffic?

MS. ECKERSLEY: It's true that we've had a long

struggle to move from a plain text Internet where we all use Telnet and unencrypted SMTP and POP to an encrypted Internet where, unfortunately, as the network grew, it just became less true that you could trust the network never to listen to your usernames and passwords or the content of your communications and do things that you didn't want done with those communications. So, all of those examples of protocols are protocols that we're trying to encrypt.

SMTP, you know, ideally should go over SSL. POP definitely goes over SSL these days really. And if you're not sending it over SSL, you're doing something wrong. So, I think the same lesson applies to the web. We've got the SSL protocol. It has its flaws. Those are fixable, I think. But it will take some work to get rid of the flaws. And, right now, flawed SSL is a million times better than a plain text Internet.

MS. SCHWARTZ: I want to know one thing. On Commissioner Harbour's list this morning, when she was talking about the email providers, she didn't mention Gmail. And that's because after the China incident, Gmail switched over to use SSL by default. All Gmail connections.

MR. ECKERSLEY: Yes, many, many congratulations to Google for doing that. They showed that it was -- I

mean, there was an argument until Google did it that it was too expensive for a huge cloud provider to encrypt everyone's email communications. And Google has demonstrated, actually, it's not that expensive anymore. Computers have gotten fast enough that we can encrypt everyone's email and still have it as a free service.

MS. LEFKOWITZ: So, one question, and sort of, you know, if you look at the -- even at the postal mail, if the post office sees white powder leaking out of an envelope, they're going to open it, right, and then they'll do everything they can to try to track it down. So, is there some role for law enforcement in tracking of data and is there some way to make those two compatible?

MR. ECKERSLEY: I would love to be able to say that just by turning on SSL law enforcement is completely disempowered and needs to go and get lots of warrants in order to access things. Realistically, that email is still stored on the cloud provider's servers and, frankly, you know, a lot of the time I think it would be not that hard for law enforcement to find a due process way to access email.

The people who are really being locked out here are authoritarian regimes that don't have a legal process way to access that cloud provider. I think Iran was very unhappy about Gmail turning on encryption because it

meant they couldn't eavesdrop on their citizens anymore, because the Iranian government couldn't go to Google and use legal process to obtain that email.

MS. LEFKOWITZ: Okay. Well, let's move up a layer. Let's talk about browser controls. So, are there any technical changes that could be developed or implemented to address some of the privacy issues that we're talking about and how easy or difficult would they be to implement and how usable are they for consumers?

Ed, do you want to start us off?

MS. FELTEN: Sure. This is an area where I think all the major browser venders are trying to find ways to innovate, to give better technical controls, to give users more effective control over when they can be tracked and linked and what information gets provided.

Historically, browsers have just promiscuously provided all kinds of information about the user, information which Peter and some of his colleagues and others have shown is often sufficient to uniquely identify a user. And that doesn't have to happen. It's not technically necessary, but it's a matter of really careful engineering in designing the browser to make sure that you're not inadvertently giving information that's useful. It's a matter of thinking about what information really needs to be released ever. It's also important to

give users more control over what information gets released and to which sites.

There needs to be a lot of change, I think, inside the plumbing of the browser and then, to the extent you're giving users control and choices, you need to think really hard about how to present those choices to them in a way that's better than we've historically presented privacy choices to users.

MS. LEFKOWITZ: Is there any work going on in that?

MR. FELTEN: Well, there's a lot. I mentioned the browser vendors. There's work that we're doing in our lab at Princeton, as well, to try to look at browser architecture and try to figure out how to let users compartment the information that's given to different sites and give users control over when sites can connect, what they do on one site to what they do in another. And that means engineering the browser so that it keeps track of where information came from and so that it's careful about which information is given to whom. And that's an issue that we're working on and also some folks involved with browser vendors, as well.

So, I'm hopeful that we'll make progress in this area. But it's a constant arm's race, if you will, between people who are trying to find new ways to track

and identify users and those of us who are trying to establish technological control over those. That perimeter that I talked about before seems to be getting larger and there are people out there who are working to make it larger.

MS. LEFKOWITZ: Okay, anybody else?

MS. LYNCH: There's a little bit of an elephant in the room here which is the user experience is user driven. And in many cases, the user will do what is convenient and what delivers to them the experience that they've learned to expect. So, in many of the cases that we're talking about, we're talking about the user making an intervention, the user making a decision, the user making a choice. And in many cases, people will make that choice once. So, it's good to get the defaults right.

In some cases, people are willing to make that choice for a trigger event that they have to be notified about. So, getting that balance right -- because, in many cases, the browsers are promiscuously sharing information so that your experience is a positive one. You get the right plug-ins, you get the right whatever without the user having to actively manage their sessions all the time. And getting that balance right is one of the big difficulties here.

MR. FELTEN: If I could just jump in briefly.

MS. LEFKOWITZ: Sure, go ahead.

MR. FELTEN: What Lucy said is absolutely right, that -- and this is one of the reasons this problem is really hard. You need to give users the experience, the benefits that they want from using the net, and you need to do it in a way that is realistic about how much decision-making they want to do and --

MS. LYNCH: And how often.

MR. FELTEN: -- how well equipped users are to actually make those decisions. It would be easy if we didn't have these problems to deal with.

MR. ECKERSLEY: So, I kind of made a point about this before, but I want to try to make it more clearly. This problem of having too many choices that are crucial -- essentially, you can imagine the innards of these browser settings as being a gigantic switch box which like allow this site to send this bit of information to this other place, allow this thing over here to talk to that. And then, as Ed pointed out, you only need to get this wrong once. You only need to allow Facebook and Amazon to link your accounts together once and, suddenly, forever, even if you chose a different username and tried to keep those things separate, they're now associated in those firms' databases.

So, the question is, okay, can we realistically expect human beings to be in there, in their switch box in their browser saying, yes, this site can talk to this one; no, this one can't? I think the answer is no, especially if we have any notion of what reasonable usability looks like.

So, the idea that I was talking about before when I talk about crowd sourcing these things is saying, well, for a lot of us, the answers to these switch box questions will be the same. It's going to be a complicated pattern of yeses and nos about which things you want to allow to talk to which other ones. But let's try to solve this problem collectively. Let's all get together in some technical process and say, okay, let's try to answer the switch box questions. And I don't know if this approach will work, but I think it's the best one we've got to try at the moment.

MS. LEFKOWITZ: I'm a very practical person. So, how does that work? I mean, who is going to sort of start the crowd sourcing?

MR. ECKERSLEY: Well, the precedent that exists right now is this plug-in Adblock Plus and some other similar ones where the model is fairly simple. It's a list of things that your browser isn't allowed to load. Some of those things are scripts, some of them are

images, maybe the one-by-one transparent JIFs that are solely there to track you, to make your browser go and fetch this tiny, invisible image from a web server just so that a server can see where you are coming from to fetch that image. And people try to compile lists of these things and say whenever your browser encounters a reference to one of these objects, just don't fetch it. So, that's a reasonable first approximation.

Now, the way -- most of the way that Adblock Plus does this is by getting human beings to compile lists and usually they target advertising rather than tracking. But I think the same model is equally applicable to the tracking stuff, which is probably of more policy concern. And then the question is, can we compile a good enough list that's long enough and comprehensive enough and has enough people looking at it and working on it that it gives people a solid percentage level of protection.

MS. LEFKOWITZ: I was going to let Drummond and then John.

MR. REED: I was just, once again, going to make this point about the difficulty of privacy by design. So, I think we all know that as egregious as cookies can be for tracking, if we put the choice in front of the majority of consumers today, you can stop

that problem, just turn off cookies, how many would do it? Even if you make it one big red button right in front of them, their web experience would suffer to the point that, you know, a tiny fraction would take that choice.

So, if we're going to solve that problem, I would submit there has to be a more overarching solution to doing it. And Peter's got a good point in talking about -- technologically, there are some ways that I would say are actually reflections in policy.

Another structural way that I think we'll talk about as we get through identity management is this emerging paradigm of trust frameworks. And I would submit they are going to be a powerful tool for being able to approach that.

MS. LEFKOWITZ: John?

MR. CLIPPINGER: I was at a conference, South by Southwest, and Dana Boyd, who is an ethnographer of sort of the web and web behavior, gave a very excellent talk on privacy. And I think she came up with a very different perspective in how to look at -- rather than doing toggles and choices and attentions. She was talking about different kinds of publics and expectations that people have in different kinds of publics, and things that are behavioral and what you call articulated.

And people are very good at social signals. I mean, the bigger part of our brain is dedicated to sort of interpreting complex social signals.

The question is, are those signals there in the environment that people can build upon, intuitively build upon, and they're constantly building new norms and inventing ways in which they create their own little publics. So, I do not think it's going to be -- I think we're just on the edge of understanding this. So, I don't think it's going to be a complex of toggles and switches. Yes, you have to have some kind of fundamental understanding, but I think that you're going to have to build on the sort of dynamic intuitions that people have and rely upon sort of cohort norms that people have. And you have to have some enforcement, you have to have some consequence or violation for bad actors.

I mean, there's so much work now that's being done in behavioral economics and trust and how it works and how implicit trust mechanisms are created and enforced and how people develop contracts and conventions among themselves in an emergent way that I think this is going to require a different way of thinking about it. And I think to prematurely rely upon techniques that have not worked in the past projected into the future will not be particularly beneficial.

MS. LEFKOWITZ: One final point, Ari, before we turn to --

MR. SCHWARTZ: Yeah, I just wanted to push back a little bit on what Drummond was saying about that privacy by design is hard. I do think privacy by design is hard if you haven't thought about it in the protocol at the beginning. And cookies is the perfect example of that, right? I mean, there was basically no thought to privacy when cookies were created and now we have to deal with the consequence of that and create this whole complicated set of controls around it and rules about how they're used, et cetera. If we had tried to build user controls in the beginning, it would have been much easier than what we have today.

So, I think there's generally a viewpoint among some technologies, particularly among companies, that says, we'll put the technology out there and we'll figure out some of -- we'll do rapid prototyping and figure out how to address those privacy and security problems down the road. It turns out that privacy and security, in particular, are much more difficult to build in after the thing's been created. If we had thought about it in the beginning, we could have addressed it much more easily.

MS. LEFKOWITZ: So, we've been already talking a little bit about identity management, but let's jump in

a little further because we've already heard that many people have said that the Internet doesn't have an authentication layer built in. So, often, people talk about identity management as a means of solving that problem. But let's make sure we're all on the same page.

Lucy, do you want to give us a little nutshell of what identity management means and what do people mean when they talk about federated identity management?

MS. LYNCH: Well, I think the first thing to recognize is that people are generally talking about that experience at a very high level in the network. They're actually talking, in general, about a web experience, although there is some work going on in federation below the web for services like data sharing. But, in general, they're talking about the end user facing experience and a relationship between a service provider and end user and somebody who is your trusted relay among those relationships.

If you think of privacy as not secrecy, but as information sharing with consent in a context, federated identity is really about allowing the user to select the pieces of information that you need to share to accomplish the service through a proxy so that only those details are shared. But it means that the user needs to move trust from themselves to the proxy. Or they need to

be very active in acting as their own proxy with these zero proof tokens.

And that, in a nutshell, is really what you're talking about, is empowering both the user and the service provider to have a successful transaction without having to do a high degree of information sharing.

MS. LEFKOWITZ: So, what will we get if we could build a good identity management system? What's it going to do for us online and what won't it do and will it even necessarily increase privacy?

Jules, do you want to start us off?

MR. COHEN: Thanks. This is another question where I think it's helpful to look back to the real world. You know, in the real world, we have this way of proving our identity in various situations, and when you ask, what will we get online, I think we'll get the same kinds of benefits online if done correctly that we get in the real world. We'll have the ability to demonstrate who we are to a service provider. The service provider can make a trust decision about us, be that Microsoft or be that the Federal government or the State government or whomever, whoever you're getting the service from. If the token that you pass is the correct level of assurance and they deem it trustworthy, you get a service back.

I want to just follow up on what Ari said with

respect to how we can potentially do it better online with an example. So, in the real world, if I walk in to a museum and I want to prove that I am a student at an accredited university, I pull out my student ID, and they can see my name, they can see the name of the university, they can probably see my -- you know, when it expires and when I graduate, and some other pieces of information. But really they need a far smaller amount of information to determine whether or not I'm actually a student. They just really need something that says, bearer is a student. It doesn't matter whether I go to Harvard or Princeton or some other school. Those pieces of information aren't necessary.

On the Internet, we can do that kind of redaction. We can share a token with somebody -- a user can choose to share a token that says, I am a student, redact the pieces of information that are unnecessary, and the relying party, the service operator, can make a trust decision based on that.

The same example we talked about it a couple times, when you go into a bar and order a drink in this country, they want to know, is it a valid ID, are you over the age of 21, and that's about it. Does the picture match? They get a lot more information. And in the real world, it's really difficult to stick your thumb

over all those extra fields and redact them. But on the Internet, that kind of redaction is possible.

So what can we get out of identity management? We can get those same kinds of trust moments that we get in the real world, but we can get them with a higher level of privacy through redaction and through the kind of unlinkability that's possible that prevents the concern about linking all those cards in Ed's wallet.

MR. SCHWARTZ: I think one important thing to note is that in this space, privacy and security are very much aligned. One of the problems that we have with security online is that too many people have information that they shouldn't have. So, that's both a security problem and a privacy problem. If we can get the right people the right information at the right time to authenticate, to use services, et cetera, that will help both privacy and security. But that means looking at the whole environment of the Internet.

And most companies, I think, are going to be somewhat -- are going to push back. I'm skeptical that companies -- what's called the relying party in a lot of these trust frameworks, that the companies are going to be enthusiastic about the idea of getting less information even though it means that the whole system is more secure.

MS. LEFKOWITZ: Ed, and then we can go down the line.

MR. FELTEN: I want to amplify that. I think it would be nice. I, as a consumer, I guess would like to live in a world where sites only ask for the information they needed to provide a service. But that's not the common practice today.

If I want to get an account in NewYorkTimes.com, for example, to read the newspaper, they ask for my gender, they ask for my year of birth, my zip code, my job title. And, of course, I could lie. But they do ask for that information. And it's obvious why they're asking me for it. It's not to provide the service. They don't need to know my gender to provide the service better. You know, it's a transaction that they offer to me. They're up-front about what they're doing. So, I don't think they're cheating me. But, nonetheless, the business practice is that sites ask for more information than they need to provide the service and that people give it.

So, you can have a better authentication mechanism for logging into that site, but still, ultimately, they will ask me for the information as a condition of using the site.

MS. LEFKOWITZ: John?

MR. CLIPPINGER: I'd like to challenge that a little bit because this is something that we worked with and talked to a number of companies about and, I mean, major financial services companies, large retailers, a variety of parties. Because the assumption would that be they can get as much information about you as they want; they're going to do that. And so, we had a working group, we brought a number of these people in. I was very surprised in the sense that they -- a lot of them do not want to have the liability of having the personal identifying information and they would like to have a trusted relationship where you would give them a lot of information that, in fact, they could really know what your preferences were.

And so, if there was a vehicle, a means by which they could get the information they really need. They don't have to know exactly where I live. They don't have to know the -- in many cases, the physical me. They maybe have what I would call a virtual me that has certain sets of attributes that are very valuable to them, that I'll carry on transactions, and have a sort of social contract or an economic contract around that that's enforceable. I think it plays both ways. I think there will be a change -- and I was very surprised to see that there is this shift that's taking place. Some

people call it the big flip. But I think you'll see that.

MS. LEFKOWITZ: I have a hard enough time negotiating with my phone company to get a better rate. So, I mean, that sounds good, but how is that going to work on an individual basis? People are going to trade more attributes for something, better discounts? I mean, are they really going to do that?

MR. CLIPPINGER: This is exactly what I alluded to earlier. Because as information starts to become valuable, then you get into this asymmetry of the bargaining position, and then there has to be a regulatory governance framework. But I think the enlightened party, what they want to do is have a trusted relationship with an aggregate of their customer base, that they get the information they need in order to produce a better product. And if there's the attempt of a provider, a service provider, to coerce or trick and trap, and this is what I fear, then I think you're going to move into a very adverse environment.

There doesn't necessarily have to be that incentive. I think they can have a better business opportunity by not doing that. And I think the trusted exchange is going to be key to building a brand.

MS. LEFKOWITZ: Did you want to answer that,

Drummond, or did you want to talk about trust frameworks?

MR. REED: Both.

MS. LEFKOWITZ: Okay, go ahead.

MR. REED: Well, first, I want to agree with John here. One of the reasons I am such an advocate of trust frameworks is I think that the building of identity management is just a first piece of this relationship layer that we're talk about. And in some ways, it's one half of the coin and one side of the coin, and trust frameworks are emerging now as the other half of the coin.

And the power is, I believe, to what Ari -- a very good point, which is how can you actually align the consumers' incentives for privacy and protection of their information and the businesses' incentives to get the information they need to best deliver the service. Really that's what both of them are incented to do. Can we align that with protection of the consumers' privacy and security? The optimist in me says that trust frameworks are a means to do that.

Now, let me make it clear what we're talking about when we're talking about a trust framework. As Lucy was explaining, the concept of identity management as we're talking about it on an Internet scale is that from a consumer's perspective, you're able to use --

identify as a service. You're using a specialized service provider to encapsulate this. I don't need a service provider to go up and show credentials from my wallet in a physical store or in a bar or something like that. But on the Internet, I'm not physically there. I can, with technology like information cards, put this service right here locally on my machine, on my laptop or on my iPhone.

But immediately you'll start to see one problem, which is, well, if it's tied to that physical machine, what if I'm using a different machine? What if I'm over at a friend's house? What if I lose one of those things? So, you're going to see that migrating into the cloud. You're going to see these credentials. Well, you're starting to suggest something that's very similar to what we have in the financial system, which is to carry out financial transactions all the time we use banks, and banks are trusted to be in that position of our intermediary with sharing that information.

Now, of course, it's a highly regulated environment for many reasons, and what we're potentially evolving here with identity management on the Internet is a class of service provider referred to as an identity service provider or sometimes identity provider, which scares me a little bit because it's not really providing

your identity, right --

MS. LYNCH: A broker.

MR. REED: Yeah, a broker. And, now, the concept of trust frameworks is in that context, fairly simple to understand, which is now you've got a service provider, an identity service provider, that's in the position of serving as your proxy or your intermediary, sharing information selectively with sites that are called relying parties. They're relying on the information that's being shared by the identity provider. But think of it this way, you've also got potentially an advocate. You've got a service writer who is in the business of helping you protect your information when it's being shared.

So, to some extent, this starts to address the asymmetry that John was talking about. When you go as an individual to a site and you're looking at a privacy policy and you have none of the technical legal capability to look at it, that's really an asymmetrical relationship. When your identity provider, which may be -- I mean, there are many examples of companies that are already looking at that business, Paypal, Google, Yahoo! AOL. They are in a position to say, okay, there are norms for these things. We can tell you what sites we've found to have the policies that are favorable to you and

which ones don't.

So, the emergent idea of a trust framework is that there's a set of policymakers that say, okay, for these exchanges of identity credentials, there are certain requirements that identity providers need to meet and there are certain requirements that the relying parties need to meet. We're going to specify those in a trust framework and then there's going to be a way to actually certify that the identity providers meet what are called levels of assurance in the credentials they're issuing and that the relying parties meet levels of protection.

And the best example is the one that's already been implemented by the U.S. government, a group called ICAM, and it's called the trust framework provider adoption program. They've actually outlined a process for the Federal government, using trust framework providers. And just two weeks ago, the first two trust framework providers for members of the American public can actually start to use commercial identity providers to provide open ID or information card credentials to U.S. government websites. And those trust frameworks, developed by ICAM and the GSA, have a set of privacy requirements in them that both the identity providers and the relying party sites need to meet.

That capability of a trust framework to set up that overarching set of agreements and not just the security, but the privacy norms, is I think a potent new tool and it's not just for governmental interactions. It can be for any type of Internet interactions.

MS. LEFKOWITZ: Well, let me ask one thing. So, this seems to introduce like a whole new privacy issue. I mean, if you look offline and you take you your driver's license and use it at the bank or the airport or the bar, it's not as if the DMV knows where you've used that driver's license. But, now, it seems as if the identity provider is going to know all the places that you are using that identity. Is that of concern? Should we be concerned about that?

MR. REED: I imagine you're going to get about six different responses, so I'll let others go first.

MS. LEFKOWITZ: Okay.

MR. SCHWARTZ: I would say, yes, we should be concerned, but there are things that we could do to address that concern. You know, the optimist in me sees a system that you could set up here that's not too farfetched, that could address those concerns where there are rules about what identity providers can do with that information. You have the unlinkability between the two different sets of the credentials that each of these

have, so they use it in two different places, they can't compare it. So, it actually provides stronger privacy and stronger security while still authenticating at a better level than what we have today.

So, I think that the possibilities are out there, and to have a federated system where you could have more than one set of tools to use in different places. So, I think there is a path out there, but it means setting up the right kind of rules and putting it in place and giving the right incentives. I think one of the things I thought was really interesting from the FCC broadband plan was they took this issue head on. They supported the idea of federated identity exactly as Drummond laid it out just there, but also suggested that there needs to be -- and they actually had a separate pullout box on this -- the idea of FDIC-like entity to oversee -- which is a private entity backed by the government to provide insurance in this space.

So, it's sort of serving as the super trust framework and setting up the rules by which if you follow these rules as a trust framework, you get safe harbor and you can -- in this space, but you have to follow the basic rules, driving people to -- and the real benefit is you have the liability protection and the insurance backing of the government, and then also, individuals can

feel more trust in it, too, because of the data portability issues and the fact that they know that there's some government backing behind this process.

So, it's an interesting model. I'm not saying that it's perfect. I mean, you still have to come up with the right rules, but an interesting model to look at. I think it sort of adds a new dimension to this discussion a little bit. And that's just brand new from yesterday.

MS. LEFKOWITZ: Peter?

MR. ECKERSLEY: So, I think there are different ways that this could go. The fundamental question is you're going to have an identity broker who's a central party that controls where your information goes. You really want to know, who does this identity broker work for? And I think there are a spectrum of answers to that. There's the worst possible answer which is that the identity broker is like a data broker. That is, they work for relying parties, they work for the people who want to know more about you, and they're in the business of giving your data to other people for a fee. That's the worst answer.

Maybe there's an answer that's in the middle which is maybe they're a bit like a bank. Do banks work for us? I mean, I think that's probably a controversial

question. There are probably some situations in which they really do work for their customers and other situations in which the bank works for itself. So, that's a murky case and talking about a data FDIC is bringing that image up for me.

Then probably the best possible case would be if this organization really works for me, then -- and there's a way that they can really demonstrate that they work for me, maybe that's a good thing, maybe that allows a bunch of trust relationships and allows me to have some competent professionals defending my identity online and telling companies that want my details before giving me an account, no, like here are some fake ones, or no, sorry, we're going to negotiate as a group for our customers and refuse to disclose things that you don't need to know. So, if we can get to that world, maybe this is a good avenue to go down. But we've really got to make sure that we're going down the avenue where these organizations work for their users.

MS. LEFKOWITZ: Jules?

MR. COHEN: A couple of observations. One, just to follow up on the question you raised about whether the identity provider can see all the places that you go. I think that -- you know, again, looking at the offline example, I think it's instructive to think about

some of the privacy principles that are inherent in the offline world and thinking about whether they can move over.

So, for example, to your point in the offline world, you know, the person who issued my student ID or the person that issued my driver's license can't see where I used it. They're also issued in a decentralized manner, so I can choose which of those IDs in the offline world I use, which is a huge thing that we need to move over into the online world. I don't always want to be using the same one.

And then this notion of unlinkability. If I use my student ID here and I use it here and I use it here or my driver's license, to Ed's point, yeah, it's possible to link them in the real world, but there's a fair bit of friction there. Somebody has to swipe it or photocopy it or write down the contents. And a lot of those transactions in the real world are femoral. Somebody looks at it, makes a trust decision, moves on, and there's no record kept. To the extent that we can try and view the online world with that principle as well, that's great.

I would note that there are some IDs in the real world where you show them and there is a record kept. ATM cards, you know, stored value cards, those

sorts of things. They have a slightly different set of principles.

The other thing I would note is just around this conversation about the various parties involved in the transaction. So, you have the identity provider, you have the user and you have the relying party. I mean, at some level, those are the core three. And one of the interesting challenges I think that we're noting here is that they all need to be accountable and it's really a very shared thing. If one party is less accountable than the others, then you have an imbalance and it will work a lot less well.

MR. ECKERSLEY: Jules, can I quickly ask you a question?

MR. COHEN: Yes.

MR. ECKERSLEY: When you talk about unlinkability, Ed made a good point before about the fact that we can make up usernames and passwords for sites and those function a bit like throwaway identities from an identity management system. But they can be linked together by all of the usual web-tracking mechanisms like cookies and third-party requests. Do these unlinkability properties that these frameworks purport to have actually really protect us against that problem?

MR. COHEN: So, I think the question is, to

what extent can the protections that we're talking about building in at the application layer, at the identity layer, actually help us in the plumbing layer? That's a question of whether those technologies can be ported down. And I guess the point I made earlier, which is that the nascent identity layer can exacerbate the problem and make it a lot worse or we can build in protection to that layer and not make the problem worse and then there can be a different set of conversations about the plumbing.

MS. LEFKOWITZ: I think Lucy has been waiting a while.

MS. LYNCH: We've actually moved on. So I'll pass.

MS. LEFKOWITZ: Ed, you wanted to answer that?

MR. FELTEN: Sure. I actually wanted to follow up on what Jules just said. From my standpoint, I think there's a lot to like about systems that help you automate the management of your identity and log in in an unlinkable way and so on. And those can all be improvements.

But from a privacy standpoint, I think it's a useful goal, in those technologies, to strive for making things no worse than they are today. Providing the level of unlinkability that you can get with passwords, for

example. But, fundamentally, I think they don't solve one of the big privacy concerns that a lot of users have and that is the kind of market negotiation that goes on in which a user reveals some private information in exchange for getting a service. You can build technologies that make that negotiation more efficient, that make the result more precise, that improve enforcement of violations. But, fundamentally, the negotiation is still going on and there is a traffic in private information that is inherent in the way that the market operates. And I think you have to step outside of technology redesign if you want to change that. And you're opening a real Pandora's Box, I think, if you do.

MR. LEFKOWITZ: Drummond?

MR. REED: I agree very much with what Ed said and I want to point out that is the sort of fundamental purpose of trust frameworks is to say, okay, so we have this selection of technologies -- and I want to make a couple points here.

First of all, no one is proposing a single overarching trust framework for the whole Internet. In fact, the model of the two trust -- and Lucy and I are sitting side by side. The two trust framework providers that were announced two weeks ago at RSA are Kitara and a new organization called the Open Identity Exchange.

MS. LYNCH: They're both only U.S. gov facing. This is not global technology.

MS. LEFKOWITZ: Can you talk into your mic?

MR. REED: Right.

MS. LYNCH: I should point out here that these trust frameworks are U.S. centric and we're talking about a global technology and global policies. And at some point, inter-federation will require that you, as a U.S. citizen inter-operate somewhere else in the world. So, this is the kernel of the beginning of a solution to a problem which is much larger. There are some European programs, like Stork, already looking at this problem, as well.

MR. REED: So the key point of the open identity exchange approach -- and there are two white papers at openidentityexchange.org that I highly recommend on this to address Lucy's very issue, which the OIX approach was to say, okay, the U.S. government has really proposed the first trust framework provider program coming from -- there's a collaboration between the Open ID Foundation and the Information Card Foundation to help create OIX. The approach was there to say there are going to be many more trust frameworks.

There are going to be trust frameworks -- one, a semi-public, non-governmental organization that's

looking at a trust framework right now is PBS. It's saying we could use a trust framework in public media to help connect all of our member stations; basically, a federation of all the member stations and also the websites that service many PBS shows. We'd like to have folks that have credentials from a PBS station as a member or supporter be able to go to shows, the sites for those shows and be able to exchange information under a certain trust framework or a certain trust expectation. That's an example that's not governmental. There are a number of other examples given there.

So, the point there really is that those contexts, as John is putting it, can be represented by a trust framework. To address the usability issue, from the end user standpoint, it's really sort of like making a decision like a financial decision. Do I trust this merchant? Do I trust this network that I'm working with, a particular credit card? If we can do that, then we can get to a set of policies that are bound to the technology being used such that you're able to establish norms for good behavior at a fairly broad basis. It is a new way of essentially binding technology and policy that I think has the usability characteristics that we need.

MS. LEFKOWITZ: So, let me ask, so we started this session by talking about what we should have done in

the beginning when we were developing the Internet if we had thought clearly enough about it. Now here we are on the cusp of a whole new system and we're talking about, you know, how it could be set up to do it right in terms of getting the benefits as well as maintaining privacy. So, how are we going to get to that could? I mean, is that going to be -- do we need regulation, new regulation? Do we have old regulations that work? What do we -- is this going to be self regulatory standard setting? How are we going to get there?

UNIDENTIFIED MALE: How much time do we have? (Laughing).

MS. LEFKOWITZ: John?

MR. CLIPPINGER: I think we have to acknowledge, at least from my vantage point, is that we're designing a new kind of ecosystem and there are precedents and there are analogies we can build upon. But I think it's very different and I think it's going to be an evolving process. I think that the proposal that came out of the FCC and FDIC kind of model where you have the regulatory as a backdrop to allowing the private sector to do things I think is an interesting way of approaching it.

I think it's going to evolve over periods of time. I think that there's going to be a lot of learning

exploration. When Drummond was talking about trust frameworks, I think there are going to be lots of inventions in that over time.

One of the things I want to mention is that we're looking a lot at mobile data, which can be highly identified. I personally think there has to be something like a personal vault that has stewardship, fiduciary responsibilities, because I think this information is very, very valuable and I think as stakeholders come in and see these are the new kind of banks, these are the new kind of business models, there's going to be a lot of pressure. And you don't want to have some of the problems we had in the financial services industry spill over here and use those precedent. That is a very big concern that I have.

MS. LEFKOWITZ: Ari?

MR. SCHWARTZ: As I said earlier, I mean, I have some concerns about how much the relying parties, the companies that would be using these services, would actively promote the idea of these services knowing that they may get less information and they may have to collect information separately. I do think that there are ways -- if we can come up with incentives to get them involved in these systems, that there are ways to give users real control, to make this user-centric as John and

others have said on the panel.

To make that happen, one of the things that we look at as sort of the background to this is to look at what we have in the world today, falling off of Jules, and looking at the Fair Credit Reporting Act as sort of a model in this space. We had a pretty detailed filing for this roundtable on that topic, but the basic idea is that we usually think of the Fair Credit Reporting Act as covering credit, insurance, and employment as sort of the main areas.

But if you look at the law itself, it's actually much broader than that in terms of really using background and reputational information for eligibility for a covered need under the act, including one very broad area called business need, which, if you look at the FTC commentary, is a whole bunch of areas of eligibility, including landlord rental issues and even dating services are directly mentioned as examples.

And I think what we're seeing in this space, when you're talking about people getting access to services or getting access to sites on the web, we're starting to see a little bit of a blur between the traditional split that the FTC used to have in this area where they said, well, if it's about eligibility, that's covered, and if it's about identity, that's not covered

under FCRA. We're starting to see that. Now, you're going to start using these authentication services for eligibility to get on to a site to make decisions for an individual. So, we're starting to see that blurring there.

I think that in some cases today we would have an argument that the FCRA applies and we make that case in the paper. Some cases, there's a big gray area where some cases are falling and some cases clearly would be out of the FCRA. But I think that the identity providers and the trust frameworks can learn from the protections that are in FCRA and build a model around that, build contractual models. The way that we put it -- in our work prior to what the FCC was talking about in the FDIC case, which we'd have to look into a little bit more, but in terms of the trust frameworks, building three party contracts between the user, the relying party and the identity provider to get -- that include levels of protection around this area.

MS. LEFKOWITZ: Peter?

MR. ECKERSLEY: If I take the question, how do we get from the Internet of today where, frankly, most of us have no privacy to an Internet of tomorrow or the Internet we might have built back in the '90s if we had had that crystal ball where privacy is there by default

and most of us have it. I think the first thing to remember is that there's no guarantee that we're going to get to that Internet. It's actually going to be really hard. The costs of not getting to an Internet that protects privacy are actually very high. There are a lot of bad things that happen when you don't have privacy.

But if we want to get to it, we're going to have to try really hard. And that's going to involve like throwing lots of kitchen sinks at this problem. We're going to have to have engineers working on fixing these protocols at the low level, but we're also going to have to have regulatory agencies looking over their shoulder and saying, are you doing a good enough job yet? We're going to have to turn around to the browser manufacturers and say, you guys need to fix the cookie settings and the third party content settings and all of these things and we're going to need to have other non-technical institutions making sure that happens. And then we may also need better privacy rules, as well.

It may be that we'll get like a third of the way by technical innovation and another third of the way by implementing better privacy rules and then the last third of the way by magic and levitation. I don't know. I think it's going to be... (Laughing).

MS. LEFKOWITZ: Drummond, are you going to wave

a wand down there?

MR. REED: In terms of specific areas of focus, again, with this version, as you put it, if the emergence of an identity management trust framework is giving us a new tool at this relationship layer, then I do want to point out one specific area, which was in the expectation, the initial sort of -- the way trust frameworks were envisioned, for instance by ICAM, it was the concept of specifying levels of assurance from the identity provider.

What that means is if you -- if a site needs only a low level of assurance that you are who you are -- a good example is the Federal government, a national park site that wants to take a campsite reservation. They don't need to know -- they don't need to deeply proof your identity. They just want to make sure if you're coming back to the site to change that reservation, you're the same person. That's called level of assurance one.

However, if you want to go and look at your tax records or health records, you're going to have to be up at at least level of assurance three. And if you're talking about government employees or defense contractors, that's a level of assurance four. Well, that's what -- these four levels of assurance were

defined by NIST and it's a very well established concept on the side of what's the level of confidence you have in the information coming from the identity provider.

When we started to look at this and say, okay, if trust frameworks are going to now be a tool for establishing policy for identity management in an Internet layer, there needs to be the corresponding concept on the relying party's side, which it was Mary Rundle at Microsoft that -- co-author of one of those two papers that I pointed out -- who said, we should have that corresponding things, let's call it levels of protection.

And that's the levels of protection to which the relying party sites, when the information is shared with them, whether it's non-correlatable identifiers at level one and they actually have to say our policy is we're taking a non-correlatable identifier, we're not going to try and correlate it. You're giving us other information that is correlatable, but at level one protection, we're saying we're not going to correlate it, okay? On up to higher levels of protection.

It solves the problem, A, of making it understandable to consumers and, B, it establishes again these norms which, as Ari was saying, if they get established in trust frameworks for which there's

societal pressure, if not regulatory pressure to adopt, that's again a tool that could solve this problem on a broader basis.

MS. LEFKOWITZ: Ed?

MR. FELTEN: I want to agree with what Peter said about the technical opportunities. But I want to add two things to that. One is that although I have high hopes for what we can do technically, and certainly we can do a better job in designing the technology to give users more effective control, there are -- some of the underlying technical problems are fundamentally hard. And this is going to be -- the technical issues here are things that we're going to be wrestling with for the longer term.

Number two, I think there's an important role here for self regulation. I think there are important areas in which we basically have some idea of where the line between responsible corporate behavior and bad actors would lie. But in some of these cases, there really is not a well established line that is agreed upon. And I think in a lot of areas it's a matter of getting people together and agreeing on some brighter line that responsible companies can agree not to cross, and then trying to generate pressure through all the means available, including pushback from users and help

from technology to try to give companies an incentive to stay on the right side of that line.

MS. GARRISON: Well, I think the answer to today's question is that this is really hard. There are some things that we can do. We can have secure URLs, explore anonymous browsing, look at browsing controls, and I gather that browser companies are doing that, deal with cookie settings, look at things like the AdBlock Plus, as Peter called it, crowd sourcing, and identity management which addresses a part of what you do when you have to have transactions on the site. Of course, wrapped up in all of this are usability issues. There are also corporate governance issues and enforcement issues.

So, it's a very complicated topic and I think that our panelists have done a marvelous job today of introducing us to the complexities and making the information very accessible. Thank you all so much.

(Applause)

PANEL 2: HEALTH INFORMATION

MR. MOHAPATRA: Good morning, everyone. My name is Manas Mohapatra and to my left is Loretta Garrison, and the two of us will be co-moderating our next panel which focuses on privacy issues related to health information. We recognize that everyone has a viewpoint regarding health information, so we expect that our panelists will engage in a spirited discussion about these very important issues.

In this panel, we plan to examine the ways health information has migrated outside the traditional medical provider context and discuss the consequences of that migration, including looking at the benefits and risks that may result from the increased sharing of health information.

Before we get started, I'd like briefly to introduce our esteemed group of panelists. Starting from all the way to my right, we have Marc Boutin, who is the executive vice president and chief operating officer of the National Health Council. To his left is Kimberly Gray, who is the chief privacy officer for the Americas Region of IMS Health. Next to her is Deven McGraw, director of the Health Privacy Project at the Center for Democracy and Technology. And to my immediate right is James Heywood, who is the co-founder and chairman of

PatientsLikeMe.

Beginning with Loretta's left, we have Deborah Peel, who is the founder of Patient Privacy Rights. Next to her, hopefully, will be Jodi Daniel, who is the director of the Office of Policy Planning. She has not yet been able to make it. Next to Jody will be Linda Avey, who is the founder and president of the Brainstorm Research Foundation. And, finally, all the way left is Stanley Crosley, who is the co-director of the Indiana University Center for Strategic Health Information Provisioning. We are very pleased to have this panel of experts with us today.

And before we dig into the substance of this panel, I just want to go over a few logistical items. As with the last panel, audience members can submit questions to this panel by filling out a question card and handing it to FTC volunteers who will be circulating within the room.

For those people who are watching via webcast, they can send their emails to the panel by emailing them to privacyroundtable -- all one word --@FTC.gov.

To our panelists, I'd remind you that if you'd like to be recognized, just turn your name tent on its end and we'll recognize you. And we're going to have to, unfortunately, keep a close eye on the time as we have a

number of topics to cover with this panel. So, with that, I will turn it over to Loretta to get us started.

MS. GARRISON: Thank you, Manas, and thank you, panelists, for being here today. We're really looking forward to this conversation.

Deven, if we can start with you, what we've traditionally thought of as health information has changed considerably in recent years with the advent of new technical and commercial enterprises. We have personal health record vendors, we have genetic testing, medical drug information sites, online health community groups. We have devices that record information and send that information back to the manufacturers. So, what is health information? Who has it when it's no longer limited to just the information between you and your doctor or you and the hospital?

MS. McGRAW: Thank you very much, Loretta. I'm not sure that the definition of health information has necessarily changed, but the context in which we see it has certainly changed. If you think about where it is defined in the law in HIPAA, it's an extremely broad definition and was purposefully drafted broadly so that nothing would fall out of it, so that essentially all the information within the health care system would be considered personal information.

But outside the context of the medical system, we might look at it very differently. So, just to give you an example, a heart rate that is taken by your doctor in the doctor's office is medical information. A heart rate that comes from your Nike heart rate monitor or your Polar heart rate monitor is still heart rate information, but we might think differently about it because it's in a completely different context. But it would still fall, quite frankly, under the definition of health care information and whether it rises to the same level of sensitivity or not is a question that's worthy of discussion by the panel.

MS. GARRISON: Stan, do these new non-traditional holders of health information raise different sensitivities or suggest different ways in which the information should be treated as far as privacy or security is concerned?

MR. CROSLEY: I really, really want to say no, but I know that that's not going to be acceptable here. No, in fact, they do clearly. The problem we have, and Deven already started hitting on it, is that even non-traditional sources are incredibly diverse. So, you're throwing in to this non-traditional category everything from insulin pumps that wirelessly transmit information back to physicians potentially to sites like

PatientsLikeMe. So, saying is there a single way to conceive of these things is very difficult.

But I think it's also very true that health information, no matter where it is, is very different than any other types of information. There is clearly a societal and an extra you, you know, a perspective that you have to consider when you think about health information use. So, I think you always have to approach these traditional or non-traditional health information stores by asking the questions, you know, are they designed to improve the health of an individual or are they designed to improve the health of society or will they improve quality of care? Will they affect privacy? Will they create harm to privacy? Those two things have to be looked at. The juxtaposition of privacy and data control in this context becomes health or even life.

MS. GARRISON: Does anyone want to add anything to that? Kim?

MS. GRAY: I think that different kinds of health information certainly have to be treated differently because they carry with them different risks. Obviously, information about a sensitive condition, that particular individual may feel should be treated with much more care. For example, the various state laws that now address things like HIV positive status or AIDS or

drug or alcohol kinds of conditions. I do believe that we need to treat health information with some kind of eye towards what the patient's really looking for.

MS. GARRISON: Deborah?

DR. PEEL: Thank you. I think part of this discussion comes up because it did not used to be possible for health information to get everywhere. It pretty much stayed in doctor's offices. And now, with so many kinds of health websites, so many kinds of offerings on the Internet, health information is not where it used to be and isn't protected. And so, I don't think we can have exactly what -- I think what someone called context specific protections. Protections for health information have to follow the data or you don't have privacy.

And in terms of being able to slice and dice which information in health is sensitive or not, the best person to do that is the individual with plenty of information about the risks of what sharing different kinds of information are. So, we're going to have to develop really robust tools to educate people about the fact that, well, yeah, on your Polar monitor, when you're just looking at your heart rate, that piece of data, in and of itself, may not be very meaningful, but combined with all kinds of other information about you on the Internet and from all the places that collect health

information already, it could have very different implications.

So, we think that the definition of health information is broad, as Deven said, for good reason and people don't understand yet how broadly it's been disseminated. And we believe, also, that part of the reasons people share health information so freely at health sites is they kind of think that they're like doctors, you know, that health sites are out there to help me with information. They don't understand that many of the websites are business-based models and they use the information, which is extremely valuable, as a commodity.

MS. GARRISON: Thank you, Deborah. That actually brings up a really good point and why we want to have this discussion about the traditional versus non-traditional context. Jodi, can you talk about HIPAA, which everybody knows, but I'm not sure that everybody really understands what it is and what it covers and what it doesn't cover and why that's relevant to this discussion.

MS. DANIEL: Sure. Thank you. I'm sorry for my delay today. First, I just want the disclaimer, I'm with the Office of National Coordinator, not with the Office for Civil Rights. They're the authoritative

source on information regarding HIPAA. So, I have worked on the HIPAA privacy rules for many years, but this does not represent the department's view.

So, HIPAA only protects health information, individual identifiable health information, held by certain entities, traditionally covered entities. These are most health care providers, health plans and health care clearinghouses which were sort of entities that helped facilitate the transactions between the health plans and the health care providers.

The new high-tech act that was passed last year did expand some of the provisions to directly hold business associates accountable for those protections. So what that means is those entities that are doing business on behalf of a covered entity and using individual identifiable health information to do that also have some responsibilities under the HIPAA privacy and security rules to protect information. But what it doesn't cover is a lot of other entities that hold health information.

Now that we're in sort of an age where we're trying to help empower consumers, make sure information and data are available to consumers, there are a lot of different organizations that are out there that are holding health information that are not covered by those

HIPAA rules. It also doesn't include some traditional entities like life insurers, disability insurers and the like, that also hold health information. So, it provides a good baseline of protections at a federal level for health information, but it is limited in what entities have to abide by those protections and what information is protected. So, it's a starting point, but it doesn't necessarily address the gamut of discussion that we're having here.

MS. GARRISON: So, the areas that we're talking about that are nontraditional, that are not covered by federal regulation that is the HIPAA -- what everybody knows as the HIPAA rules, instead default to the FTC Act, Section 5, which is fairly broad, very baseline coverage.

So, Deven, does the context of the new non-traditional holders of health information raise different sensitivities or suggest different ways in which the information should be treated as far as privacy or security is concerned and should there be some extension of the baseline that's in the HIPAA world that extends out to certain of this information in the non-traditional world?

MS. McGRAW: Not withstanding that we agree that there needs to be baseline protections that follow

data wherever it goes, we do not think that the exact same rules should apply for data in the health care system as data that's held by commercial entities, specifically because the business models are completely different.

Now, I will acknowledge that there's some gray area here where there is sort of mixed health care mission and business model approaches out there. But for the most part, for information in the health care system, those entities use it to fulfill a mission, to care for you, to pay for your care, whatever those health care clearinghouses do, which I'm still not sure. But there's a mission that's related to health care and, therefore, the HIPAA rules were specifically designed to allow information to be used for traditional health care business operations, caring for patients, paying for care. That's not what Internet companies do, quite frankly. They have a business model to follow. And to some extent, they care that the service that they're offering through their site is seen by consumers as valuable, but their bottom line is to make money or else they wouldn't be putting the site up there.

So, to the extent that the risks that consumers face are quite different, you need a targeted regulatory regime in order to meet that. And notwithstanding that

the unfair and deceptive trade practices authority under the FTC is helpful in this regard, it's not a comprehensive framework of privacy protections based on fair information practices that HIPAA is. So, we can quibble with HIPAA at its margins, but my sense is that it's, in general, the right approach. We need sort of a similar set of fair information practice rules that govern consumer privacy on the Internet and that would cover health information as it flows there.

MS. GARRISON: Jamie, do you have any thoughts to add?

MR. HEYWOOD: Well, I want to go back to your original question where you asked us to define health information and I think this is the crux of the problem. I mean, it's very straightforward in sort of the existing health care infrastructure to define health information as a transaction between a health care professional, someone who is paid in a health care context, and a patient. And that's a very tight definition and it works.

If you go beyond that, I think we have to actually ask a little bit about what the consequence of the information is and what it means. And health is defined at some level -- could be defined and should be defined as broadly as the deviation from normal. Whether

that is positive or negative.

So, for instance, I have my own genome done, I basically have no risks for anything that's detectable. So, if I share that information, I can lower the cost of transactions I engage with in the world because I have an advantage. But my sharing that information puts everyone that is unwilling to share that at a disadvantage. So, I'm sharing a positive outcome, or you could look at that in the same way as an intelligence test, which modifies health outcomes, or any variable that is measured, whether that be heart rate or anything.

So, the question about that is, given that any information about someone, their behavior, their status either at a molecular level or at a behavioral level or at a phenome level, is useful information for someone in a competitive environment, in a bargaining environment like we talked about earlier. I don't know how you tightly define health care information outside of the business transaction process of the health care profession itself.

And I think what is interesting -- and clearly we know an immense amount about our patients at PatientsLikeMe because they share that information as best as we can in a consented and understood environment. But I would argue that Yahoo! or Microsoft or Google know

far more and could use that information with different levels of restrictions. So, I think we need to look at, fundamentally, what is the consequence of this.

If I could put one more quick frame on this, what I get concerned about when we talk about using health information in a privacy context outside of the health care professional world is, we're really starting to talk about the regulation of the flow of information and speech. We're starting to put a restriction on individuals' ability to communicate with each other in the context that they choose in a democratic fashion, with or without, more or less, effectively with consent in that process.

And we're not talking about the fact that we are supposed to live in a society that was founded on the principle that all are created equal and we're not talking about the protection of deviation from equality from discrimination. We're talking about the inhibition of knowledge about deviation from equality. So, again, we are framing this dialogue not in the consequence of discrimination space, not in the all are created equal under our principle of law space, but that we shall not communicate any deviation from that principle.

So, it's a very dangerous space here because health information is fundamentally anything that we know

about you that affects your future. And if we define it this way, we're talking about imposing a framework that comes from historical contexts that are not really appropriate for human society in dialoguing around this concept of equality and discrimination.

MS. GARRISON: Thank you. Linda?

MS. AVEY: Yeah, I think that sort of a corollary to that, what Jamie just said, is we should really, I think, spend more time defining the harms that could come from this. I think we talk about privacy and we don't really spend enough time to think what truly could happen if someone got some of your information. Let's really carry that through to an end point that would be harmful to that individual. And until we do that, I feel like we talk in a vacuum.

We got this a lot when I was still at 23andMe of, oh, if somebody gets my genetic information, let's parse that a bit, let's talk about what would happen if someone got your genetic data. Could they really hurt you in a very specific way? And when you really dive into that and drive to some points, yes, there are some concerns and we think this is why GINA was passed. That was kind of the first step to help protect people through their employers or health insurers from discriminating against them.

I think there are going to be a lot of unintended consequences from GINA that we haven't really talked about. One of the things we sat and thought about, like let's say you interview for a job and the people who interview you, they just really don't like you and they don't think you're going to do a good job, so they don't hire you. Could that person come forward and say, you know, they found the genes for being an asshole? I'm genetically an asshole and you discriminated against me for that. I hate to use the language, but -- excuse my French. But that's exactly the kind of unintended stuff that could happen if we have too many laws in place that prevent the free flow of information. So, defining harms, I think, is a very important thing that we need to do and spend time on.

MS. GARRISON: Well, I agree with you and we want to do that, but one thing from the consumer perspective is that when they deal with their doctor and they know about HIPAA, what their understanding is that there are certain protections, including security protections, around the use of that information. What they don't realize is that there are limits to that. And once you step outside the doctor's office, all of those protections, including the security protections and requirements, disappear.

Yet, Linda, in your work with 23andMe, you actually imposed those pretty strict regimes around that information in order to provide those protections that was voluntary. Do you want to talk about why you thought that was important to do there?

MS. AVEY: Well, in the world of genetic, I think it's a very specific set of issues around genetic data because if you talk to a genetics expert, they will say that if I had about three points in your genome and a little bit of phenotypic information from you, maybe from Google searches, I could identify you very quickly. So, that whole idea of de-identification with genetic data is kind of a myth. So, for that reason, we felt it was very important that we protect the information to the umpteenth degree.

You can never guarantee complete privacy, but we do feel like there is so much value in that information. But keeping it in a secure environment and then allowing people to come to you to say, you know, if I could, my dream would be to pose this question or this query against the data, allow that to happen and then spit the results out.

And in one of our conference calls, I guess this is very much along the lines of the census where the information is protected, but you're allowed to go in and

do queries of it and get some very meaningful, aggregated information back. And that does seem to be a model I think that probably is better in the genetic space.

MS. GARRISON: So, if I hear you, what you're suggesting is that there is, in fact, a place for certain kinds of rules of the road or certain minimal protections in the privacy and security around the information. Is that right? I mean, you're not saying that this is just all up for grabs?

MS. AVEY: Exactly. Well, and I should put it out there that I don't speak for 23andMe, but in my mind, it's important for companies to put out in their privacy policies what they plan to do with the information. And you should read a privacy policy very carefully before you sign up for any type of service that's going to have your personal information.

But on the same token, a lot of companies make the choice that here's what we're going to do internally, but then you also should have access to your data, I believe. And if you want that, it should be within your right to do what you want to do to share it with other people. So, if you have Alzheimer's disease or you have it in your family and you've generated your genetic data, you know what a company is going to do with it, but you want to take it and share it with other people who are

going to do different things with it, I believe that should be within your rights.

MS. GARRISON: Deb, I know you've been waiting. If you can briefly address it, we want to move to the harms.

DR. PEEL: Sure. What I wanted to say that's foundational to this discussion is the problem with the protections in the HIPAA privacy rule was the key consumer protection was removed in 2002, and this continues not to be widely known or reported. But prior to the amendment to HIPAA, consumers had to be asked for their permission before their information was shared electronically with providers.

Today, because the consent provisions were removed, all of the covered entities can make the decisions about using our information, and until we get the audit trails, which were in the high tech bill, even without our knowledge and we can't refuse or stop these transactions. So, although I agree with you, Deven, that there are a lot of problems with how health information is used outside of the health care system, many of the players inside the health care system are using our information and misusing it in ways that we would never agree to because we don't control it.

For example, all the pharmacies in the United

States are data-mined and prescription information is sold daily and used in various ways that the public typically doesn't know about or agree with. So, it's really important to understand that the key consumer protection was taken out of the privacy rule and that does make a difference because many health companies and health IT vendors are using the data and selling it for things that people would not agree to.

And the point really is, as Linda says and really, Jamie, I think as you say, is that people should be able to make choices with personal information. We just believe that everyone should know what the consequences of the choices are and be freely made. And potentially with genetic information, if you make a choice to share it, it could harm other people. So, there may be some differences with that compared to other kinds of health information. But we need entirely new tools that inform people about how the information can be used and how to control it in a way that makes sense to them.

MS. GARRISON: Great, thanks. I'd like to turn to the risk issue and, Marc, if you can lead us off. Are there new security or privacy concerns that are raised with respect to the disclosure of this information in these non-traditional settings? Are there particular

risks associated with certain information and lesser risks associated with other or other contexts?

MR. BOUTIN: Thank you. There certainly are risks, but I want to be clear to the earlier discussion. We've been focusing in on risks, but there are also benefits. And I think we need to identify and stratify the risks and identify and stratify the benefits.

The National Health Council represents 133 million people with chronic conditions, many of whom have multiple chronic conditions. The reality is they're making tradeoffs in their lives. The technology and information boom has made life very different for many people with chronic conditions. Many people who had death sentences can now live a life with a chronic condition, can live at home, and can use some of this technology to make life better for themselves.

I would grant you that there is a complete lack of understanding amongst the general public and certainly amongst people with chronic conditions about the risks here. But many of them are making very calculated tradeoffs to live at home, to live a more independent normal life with the technology that is available to them. So, clearly, we have risks. I think certain risks are more dangerous or potentially more harmful to people than others, but there are a lot of benefits and we have

to look at the risks in the context of the benefit to the individual.

And so, the challenge here is how do you stratify that risk, how do you stratify that benefit, and how do you address what are, in reality, very extreme viewpoints? When you look at people with chronic conditions, as much as 30 percent are happy to have their health information used if it's going to benefit their children or grandchildren in terms of new treatments. But on the other extreme, you have people with chronic conditions who do not want their information used unless they provide consent, and many of whom would say they would not provide consent.

The reality is the majority of people with chronic conditions, like the majority of people in the general public, fall somewhere in the middle. So, our challenge is, again, how do you stratify the risk, how do you stratify the benefit, and how do those competing interests weigh?

MS. GARRISON: And, Marc, you've mentioned, also, that when you're a patient with a chronic condition, you're balancing a lot of different things in a very different way than the ordinary individual who does not face those life threatening or life impairing problems. Do you want to speak to that?

MR. BOUTIN: Sure. If you look at an issue from the perspective of -- and we do this often in Washington, DC -- you look at a young staffer up on Capitol Hill. They may have never taken a prescription in their entire life and their perception here is very concerned about privacy and security. But if you take the context of somebody with Alzheimer's or somebody with a complex autoimmune disease or a neurologic condition, somebody who may be facing death as a result of their condition, their tolerance for risk changes. And they articulate this in this phase.

Even when you look at the risk of privacy and security breach, which I have to be very clear, they take very seriously. Nobody with a chronic condition wants their privacy or security breached. However, they'll tell us in focus group work and in other studies we've conducted that they liken it to what happened after 9/11. We all faced greater security in travel. We all faced greater invasions of our privacy as a result of that.

If you have a chronic condition and you know that you do not have a viable treatment and you know that your children or grandchildren may face the same fate, you're very concerned about the development of new and better treatments for them. You're very concerned about their lifestyles being better, being able to stay at home

longer, having better cognitive skills. And as a result, you're willing to trade off some of that security in that space. And many of these people will say they'll do it without even being asked. So, our challenge is, again, how do you balance these competing interests?

MS. GARRISON: Right. And those kinds of tradeoffs would not necessarily be made, as you indicated, by someone who's not facing those life threatening situations.

Deven, can you speak more to this point on the risks, particularly in the context of the merging of health information that's collected in the non-traditional context, merging with online or offline data that's other than health information? Because we're seeing a lot more of that merging of data.

MS. McGRAW: Yes, we are seeing a lot more of that. I want to start off by responding to some of the earlier remarks. I don't think we have to nor should we go down the road of a Draconian set of rules for consumer privacy on the Internet that essentially cut off the data flow and decrease its utility to people for the reasons for which they seek it out on a regular basis and increasingly so every day.

On the other hand, one of the harms that could result of allowing this sort of wild west environment to

proliferate is that we, in fact, decrease people's trust in going there. So, folks who have no qualms at all about having their information shared won't be deterred at all from using the Internet because there's sort of a threshold for privacy and the extent to which they care about it might be quite low.

But I'll put on the table that for most people, they actually would like a sort of baseline set of rules and many of them, in fact, think they're out there and exist when, in fact, they don't, rather than just leaving it to the privacy policy of the company.

We actually have on this panel today companies that have done -- that have recognized, in fact, that people do care about this, and so, they put in their privacy policy very clear provisions about how that data is going to be used. But that is absolutely not true for many of the sites that you see out there. And so, people are sort of in this environment where their data can be sold. If the company says in its privacy policy they won't sell it, then, of course, they can get in some trouble with the FTC if they violate that. But there's nothing that says that they have to make that commitment to people.

So, oftentimes if they even say that -- you know, the provisions of the privacy policy become very

hard to read, and so, we've got this environment where people are putting health information on the Internet, probably thinking their privacy is more protected than it is. And at the same time, that data is being merged with the plethora of data that is out there on the Internet about how much you paid for your house, things that you've purchased. And there are Internet-based companies arising all the time that are merging this data together and selling it.

We just sat in an office yesterday at CDT and pulled up a profile on me where someone was trying to sell a credit report. This is not an official credit reporting agency, but it was obviously a collection of data points about me on the Internet that had my zip code, it reported that I was married. So, part of it isn't factually true. So, the other damage here is that, in fact, this information created by data points based on your searches, et cetera, is not, in fact, always all that accurate.

But if you're merging that with true health data that people have put up there or that they maybe have put into a personal health record, then you've essentially got, again, just this incredible database of information that if we don't have basic protections in place about how that's used, that are both about how

individuals consent in a privacy policy or in a notice of practices, but is also about stopping patently unfair or unreasonable behavior.

MS. GARRISON: Jodi?

MS. DANIEL: I agree with a lot of what Deven was saying. From our perspective in promoting health information technology, we're obviously trying to leverage the benefits that you can get from making information available to other providers to improve coordination of care to consumers so that they can better manage their own health and health care, et cetera. And I just wanted to try to tease out some of what we're talking about with privacy and security because we keep kind of lumping it together.

It seems to me that at least folks sort of expect that there is some basic level of security protections that folks can't necessarily, even if they want to make their information available to some folks for research purposes or to other consumers, that there are some basic security protections so that it's not a free-for-all, that only those who are authorized to get access to the data do.

So, I think there's sort of the security issue in protecting the data and then there's some of the privacy issues. In the consumer facing services on the

Internet, we talk about privacy policies and even entities that do try to do a good job of communicating their privacy policies to consumers. We know that many consumers don't read them. Even if they read them, they don't understand them, even if the company is trying to be clear. And there's still a significant disconnect in the understanding of consumers and how information is flowing, what protections there are or aren't and what they are agreeing to.

So, I think there is a lot of room for improvement in the area of transparency and making sure that consumers are making informed choices if, in fact, they are making choices, or at least know what they're agreeing to when they put their information out there. And it's very hard to get to a place where you have consumer choice if you don't have that understanding and that transparency. So I think that is an area where I think a lot of progress could be made.

MS. GARRISON: Stan?

MR. CROSLEY: I agree completely with Jodi. I think that was very well said.

The other point I wanted to address was the trust point because I think trust is absolutely pivotal in health care for sure and non-traditional settings, as well. But think of trust not only as trust on securing

the information and the privacy protections, but also think about trust as an outcomes perspective. If people are going to a site or going to a non-traditional using their home health care devices, and they're not going to trust that the information is going to be used to their advantage or used to benefit their care, or if their quality isn't improved, their quality of life isn't improved by the sharing of that information, then they're also going to lose trust in the model that they're participating in, both the non-traditional as well as the traditional health care settings.

So, trust has to also be measured not just in -- we have to do everything possible to make sure that the information is tied down, but also we have to make sure that the information is utilized to the benefits of the individuals. In some cases that means sharing the information. And that is really precisely the issue that was faced when HIPAA was first passed. And in 2002, when they took out the consent provision was so the information could be shared and quality of care could be addressed.

So again, I don't dispute for one second that that decreased the potential of privacy protection. It's hard to argue that it didn't. But I think it also had an order of magnitude improvement in quality of care that

came about that. And so, I think that trust element is really a two-edged sword, as well.

MS. GARRISON: Marc, did you have something you wanted to add?

MR. BOUTIN: Quickly with respect to the benefits. I said earlier there are 133 million people with chronic conditions in the United States. Most of them have multiple chronic conditions. The challenge that many of them have is that when you have a chronic condition, it's usually not visible. And when you think of that number, that's nearly 40 percent of the population. So, if you count the people around you, four out of ten probably have a chronic condition and you're not aware of it and they're not aware of the other folks with chronic conditions.

One of the spaces that this new technology fills is it brings these people together online and you can't underestimate the value of that to people who feel invisible, people who are sitting in this room and feel invisible. There's important social and health and other benefits in this space. So, again, the value here is to look at those benefits weighed against the risks and figure out a solution that addresses both security and privacy, but doesn't undermine the benefits to the point where they're of no use.

MS. GARRISON: Deb?

DR. PEEL: As the only one on the panel that's a practicing physician, I think if you all were in my place -- and I've been a mental health professional, a psychiatrist and analyst for 35 years -- you would understand where I'm coming from and why I founded Patient Privacy Rights. And that is that from the moment I went into practice, people came to me and they said, if I pay you cash, will you keep my information private? Why did they say that? Because they had lost a job or their reputation had been damaged because what they said in the doctor's office did not stay in the doctor's office. And so, these are very real, very real problems, the lack of privacy, that keep people from getting treatment.

And it's not, of course, just job discrimination, but health information is used by insurers, not only health insurers, but life insurers, even property and casualty insurers. And banks and financial institutions today are permitted by Gramm-Leach-Bliley to handle and transfer health records in the same way that they share credit reports.

So, this information has gone way, way, way beyond the doctor's office. And it's really important, I think, in this discussion that we don't act like this is

an either/or situation where we must share all of our data to get the benefits or, you know, we have to Draconianly not participate at all in the benefits of health technology, and it's a completely false opposition. We should be able to do both to the degrees that we want and I don't know anyone -- if you were thinking of me, Deven, I don't know anyone who wants Draconian rules. I think we need to have choices that people make because there are significant, significant majorities that want and expect these choices because of the harms.

And we already know from HHS findings that 600,000 people a year refuse to get early diagnosis and treatment for cancer because they're afraid the information will leak out and affect them. Two million in my field, mental health, refuse to get early diagnosis and treatment because the information may harm them. And I can say this again as a psychiatrist, we have to give our patients Miranda warnings almost. Look, if you use a third party payor or if you get a prescription, this is going to have consequences for your life. And that's very discouraging to have to say that. We shouldn't have a health care system where you have to worry about whether you get care is going to destroy your future and your life.

MS. GARRISON: Thank you very much. We can clearly spend a couple of days on this, but we are a little tight on time. So, I'd like to move quickly to a topic about marketing, use of health information for marketing.

Kim, marketing or advertising is a major source of revenue for online companies. It's been permitted under HIPAA, although there were additional restraints imposed on medical marketing. Can you talk about the marketing aspects? And, Jodi, if you could also follow?

MS. GRAY: Yeah, I'd be happy to. I believe, though, that most online marketing does not take place in the HIPAA world. In other words, I think covered entities and business associates are not, for the most part, doing online marketing. I spent many years at a health plan and the marketing that was typically done there would have fallen outside of marketing. In fact, it really wasn't marketing as that's defined under HIPAA. What it really was was offering goods and services that were health related and were of direct benefit to the patients receiving that information, typically by mail. So, I'm not quite sure how the HIPAA high-tech world comes in to play here.

High-tech clearly has made some amendments to HIPAA as far as this definition of marketing goes, but,

again, I'm not really sure where that came from because I don't believe there were a lot of complaints about inappropriate marketing in the traditional health care setting. I don't believe that HHS was receiving complaints about marketing being done by covered entities or their business associates. So, I'm not real sure what the legislative intent was behind that switch to make the modification under high tech.

But, clearly, I think online marketing, the use of cookies, targeted markets while surfing the web or whatnot are not coming from the traditional health care world. They are coming from the more non-traditional kinds of things that we're looking at today.

I don't know that there is a good remedy for that today, but I'm not so sure there needs to be one. I think studies probably need to be done to see if people actually want to be marketed to through targeted marketing first, and I don't believe that's really adequately taken place at this point in time. I mean, the plus to this is that none of us really want to be bothered by marketing ads that have nothing to do with what we're interested in.

Do we welcome those marketing ads that do have something to do with what we're interested in? Perhaps. I don't know and I don't honestly know. Perhaps others

on the panel know if there has been any real research done into this, but I believe that that's probably the first step.

MS. GARRISON: Jodi, can you talk briefly about why Congress put restraints on marketing within the HIPAA context? And then we'll move to the broader online marketing.

MS. DANIEL: Sure. Well, I can't talk to Congress' specific intent, but I can talk about what were some of the rules and where the challenges are and what has changed in high-tech. HIPAA does generally require an authorization by a patient for use or disclosure of health information for marketing purposes. The challenge is, what is marketing? And something -- it's something that is related to the treatment of the individual marketing. When is something treatment, when is it marketing?

So, for example, if a doctor sends out a refill reminder, they're, in effect, trying to encourage a patient to spend more money on a particular drug. Or if there's a new drug that hits the market and they send out information to a patient that might benefit from that new drug, again, one could argue that's marketing, but one could also argue that that is a doctor trying to help provide the best treatment or inform their patient of

treatment options.

We've had so many discussions on where do you draw the line between treatment and marketing and making sure that you're preventing an entity from doing those things that are marketing that folks are concerned about, but not interfering with important treatment communications. So, the privacy rule originally tried to do this and draw this line and say that health-related communications were basically exceptions from marketing, and I'm saying that in a very general sense.

What the high-tech act did was go one step further and limited what health-related communications could be considered a health care operation and not require an authorization by saying that if a covered entity received direct or indirect payment for making the communication, then they have to get an authorization from the patient to do that.

So, there's still the question of what's payment and the Office for Civil Rights will come out with modifications to the HIPAA privacy rules or proposed modifications that will address those and ask for comment. But what the concern was, I think, is that if a doctor is being paid to make a communication, is that somehow different, is the consumer who receives that going to trust their doctor and not understand that there

might be a conflict of interest there because they're getting paid for it? That being said, a doctor in a small practice in a rural community may really feel that it's important to communicate information to a patient, but may be operating on small margins and may not have the resources or want to spend the resources to make those communications given other competing demands.

So, there may be some important payment for communications that the doctor may want to do. And so, the question is, again, what is the line of marketing? But I think that there was some concern that if a doctor is being paid to make the communication, even if it's being reimbursed for their costs, that it might taint -- you know, there may be some conflict of interest and the patient should be aware of that. I think that was the intent.

MS. GARRISON: So, Deven, there is some line drawing in HIPAA, but there's no real line drawing outside of HIPAA, in the non-traditional world.

MS. McGRAW: No, no. Again, we live in this space where we've got a set of rules that apply when information is in the health care space and those rules don't apply and we've actually argued that the same rules should not apply. Again, we've got to have a regime that appreciates the value of the Internet, but also deals

with the risks.

But in the online context, with respect to targeted behavioral advertising -- and CDT has written a fair amount on this -- essentially there aren't any hard and fast rules, again, beyond what might be in a company's privacy policy, which, of course, they then have to abide by. But they don't have to do one of those in the first place or make any specific promises. So, what you see is an increasingly sophisticated attempt to be able to target people with very specific advertising based on their click stream, all of their Internet traffic essentially, you know, pseudonymised, not that they know it's Deven McGraw, but they're able to sort of know that it is me, this single person, looking at all of these searches.

MR. HEYWOOD: And that you're married.

MS. McGRAW: What?

MR. HEYWOOD: And that you're married.

MS. McGRAW: And that I'm married and that I live at zip code 20004.

But right now all that we have to regulate the space is some self-regulatory principles that are not uniformly adopted by all of the companies in the space. And we posit that self-regulation is not, on its own, enough to protect consumers in this space. That,

instead, you need some baseline rules for which patients -- patients, I'm still in the health care context -- that individuals, at a minimum, ought to be able to, if it's non-sensitive information, be able to opt out through very clear choices presented to them. And if it is sensitive information, of which we've put health in there, which gets back to our conversation earlier about that pesky broad definition, that people ought to be required to opt in to receiving those ads.

So, therefore, you set up a situation where people who want to be targeted, who would rather not have the barrage of ads that don't have anything to do with them and would prefer to see ads that are much more relevant to their lives and what they apparently care about based on what they search for on the Internet, can do so. But those of us who don't, don't have to.

MR. MOHAPATRA: Thank you very much. I think we're going to just shift gears slightly, but in a very related sense, and talk about consent generally. And I think Deborah already spoke, in some ways, about the consent in the traditional medical environment based on the 2002 amendments to HIPAA. But I would like to ask her how should consent be addressed both in the traditional medical setting and in the non-traditional medical setting?

DR. PEEL: Well, obviously, most people in the traditional medical setting, patients, certainly my patients, and then all of the organizations that have joined our coalition, which represent 10 million Americans, believe that control over personal health information is essential unless otherwise required by narrow statutory limitations, or exceptions, excuse me.

So, we think that consent is really the foundation of trust in the systems and we're not going to have trusted Internet systems again unless people control personal information. If we look at the broad frameworks that were devised, I think actually first when it was the Department of Health, Education and Welfare, the Code of Fair Information Practices set out general principles for all personal information anticipating not -- I don't think they could have anticipated back then what we have now, but they were beginning to anticipate the problems of ease in dissemination of information and the ability to analyze it that computers brought.

So, we really think that we need in this nation something like that. We didn't think there was anything wrong with that scheme. We need fair information practices for all personal information, particularly because it's very clear that all this information about us is very valuable. And whose asset is it? Whose asset

is it? It should be that individual's asset to control.

And what's so important about this discussion is that in health care, we have the one area, the one area in life and in commerce where individuals have very strong rights and have had them since the founding of the nation. This is the only area where we know because of Hippocrates that we really are supposed to be able to control our information. So, if we don't protect these rights in health care, we're not going to be able to get them in wider commercial situations.

And you all know I think that the regimes in Europe are quite different. Even collecting an IP address is considered taking personal information. And they're not allowed to have secret databases that collect your information. I think we're going to need to be moving more to fit in with a world where individuals control digital information, data, about them.

MR. MOHAPATRA: One of the things that's come up in the previous roundtables and has already come up today is about how you get to express informed consent. You may have the fair information principles and you may have a voluminous privacy policy, but do consumers -- do patients understand what is being done with their information?

I'd like to actually direct this to Jamie right

now because I know that your company has tried very much to be very open in regards to what you do with the information. I think though, you would agree, that some percentage, however small, may still not understand what do you with that information. So, how do you get to expressed informed consent?

MR. HEYWOOD: I think the word “transparency” that’s sort of in vogue today is actually the critical element here, which is can you -- do you communicate everything as best you can? And I actually think this is important when we think about a new context like the Internet sites like us or the ones that are less transparent. You do have to think about what we’re comparing ourselves to. I think when you look at the existing health care system -- and we’ve talked a lot about business models and making money and the influence of these things on behavior. I mean, the health system itself makes money. It makes money with mechanisms that are extremely inappropriate and unaligned with patient interests, and there are all kinds of counter-incentives, almost bribes in the system, to create bad behavior on the part of health care professionals that, in general, resist them remarkably.

And so, I think in this context of transparency, you know, you really want to say where is

your cash flow coming from, what are the components that align to that, what are your goals and intent? And for us as a company, we've been doing a lot of research on this question and we actually just did -- we do research on several things. One is, do people understand what we're doing? And the answer is it varies from 70 to 90 percent based on how we ask the questions.

There's dialogue about it on our website. There was a great thread when someone came in and missed the fact that we had this page -- this line on their front page. If you're a life sciences company, learn how you can buy our data here. And they said, what, you're a for profit company and you sell the data, and the community responded. There was 121 threads posted. They were 20 to 1 all positive, you know, if the life sciences company wants to buy my data, they care about me. One line said, if a pharma company wants to buy my data, they care about me more than my doctor because he doesn't want to know.

So, I mean, there was this sort of very positive vibe in that in this context of sharing. But then we go and we ask harder questions. We just did a survey and we asked questions, would you share your Social Security number, would you share your insurance policy? Social Security number helps us find out if

people die because we don't know when they die and that's an important variable for us in looking at whether drugs work or not. You know, income, race, living situation, relationship status.

And we asked the question two ways. Would you share this information? And then we said, would you want to find other individuals using this information? Because we're trying to put that in context. And the numbers came back remarkably high. I mean, 60 percent or so wanted -- with the exception of income interestingly. Everything else they were good with; income they didn't really want to share. And we're trying to learn what's the right balance and it's listening to this sort of very democratic, open institution that, by the way, when we screw up, they tell us. But I don't think the world operates that way.

And you had asked a question earlier about rules, are there rules in principles? We don't know them yet. We have a set of values, patients first, transparency, no surprises, that we will never meet. There's no way for us to have 60,000, 100,000 people understand. It's not possible. I will say we are, I think by measure, better than anyone else I've ever looked at, but we are probably a long way from what I would define as consent.

I don’t know what the rules are. The rules are a set of principles that you iterate towards and the commitment to measure it and maybe the willingness to put that data up online. I don’t know the answer yet. And we’re moving towards that answer.

So, I think this consent question is really tricky and it does come down to trust. It’s about are these institutions acting in responsible, trustworthy manners that are aligned. And I don’t know how to regulate that.

MR. MOHAPATRA: Marc, do you have some thoughts on this?

MR. BOUTIN: Yes, thank you. Consent is really, really tricky and I would agree with some of the comments that consent is intricately linked to trust and there is clear evidence that there are many people that forego treatment as a result of not trusting that their information is going to be held confidential, especially for stigmatized diseases and conditions. But consent isn’t the magic bullet here. And that’s the challenge.

Consent, when you look at people with chronic conditions specifically and with the general public, 75 percent of people don’t understand it, don’t understand how it works, don’t even realize that they have given consent.

I'm sitting here and I'm looking at a lot of people. You guys look pretty smart to me. How many people have signed the consent forms when you went into your doctor's office? Raise your hand. How many of you actually said, I'm not going to sign it or I want specific exceptions? A couple of hands went up. That's the most I've ever seen when I've asked that question. And it's because it's very challenging.

Most people with chronic conditions are told they're not going to get care if they don't sign the consent form. The reality is the current system is not working. I think there are a lot of things that can be done to improve it. There's no question about that. And we should strive to improve it. It is interlocked with trust.

But the reality is that people expect our government to protect us in terms of public health, safety. They expect research to be done to improve treatments. We're spending over $30 billion a year with government money to figure out how to address new treatments. These perceptions are juxtaposed against each other. We want consent to be the key, but yet we want the information to be used for certain purposes. We've got to do both and I think that's the issue. Consent is, in and of itself, not the solution, but it's

part of the solution. And you've got to look at it in a greater context.

MR. MOHAPATRA: Deborah, we have just a few minutes, but if you wanted to make a quick point?

DR. PEEL: Sure, sure. Well, the problem is for the public they really do object to having their information used without their permission. Alan Westin did a survey for the Institute of Medicine and found that 1 percent of the population only would agree to open access to data by researchers; 38 percent would want to know what the project was about, the purpose, who was doing it and so forth, whether it would help their family; and another 13 percent said flat out, even with information, they didn't want digital information about them used. So, this is very important.

We don't believe that the entire public knows what public health uses are, knows what quality research is, knows what comparative effectiveness work is, knows what patient safety work is. These are all research to them and the public does want to participate. Many people want to participate. And you'll get fuller, better data when they understand that the data is not going to be forcibly taken from them and we don't need to do that.

Particularly, as a psychiatrist, I'm very, very

aware of people's mental state and what they can understand and when they can understand it. And you all are certainly right, there are people that when they're in the throes of illness or they're ill or they have some kind of impairment or they have a guardian, they cannot give consent. But the majority of people, the majority of the middle really want it and are capable of understanding what's going to happen to them if it's explained to them.

Another benefit of technology is that the technologies, independent of when you're sick, we can have robust consent tools that explain these things at a time when they're not so sensitive and explain the implications of different choices. So, we need to have a whole lot better training about consent and we can make much better consent because of technology.

MR. MOHAPATRA: Linda, do you have --

MS. AVEY: Yeah, just a quick comment about this concept of consent. We tend to talk about it, I think, in black and white. Like you've either consented to something or you haven't. But with technology, I agree, Deborah, that we now with the ability to have a consent dialogue going with people, that we can have them consent and they can change their minds.

Some people look at PatientsLikeMe when they're

not sick and say, I would never share my information, and then they got ALS and everything changes. Their life is flipped upside down. And, now, suddenly, sharing information could be very valuable to them and their families. So, this notion that we're going to define this and then everyone is going to agree to it, that's never going to happen either because we're human beings, we change, our opinions change, our perspectives change.

One of the things that I think we could focus on is how can we put language in very simple terms for people to understand as they're going through life and they're changing and they're saying, you know, I do consent to this now. But by consenting to this, what does that mean? Can we come up with standard language that people understand and companies can agree to that say, here's what you're agreeing to right now at this point in time, with this decision you are making sure of this information. Whether it's a little language on the top of a survey, but something that really triggers that trust, that people say, okay, I'm going to do this, but now I know this is how my information is going to be used.

And if we can come up with that language and that methodology, then I think we're going to make some headway. But otherwise we can't live in a black and

white world.

MR. MOHAPATRA: Well, this issue of consent is an important one and pervades all issues related to health information and privacy, and specifically to our next topic which is about the role of medical data in research in terms of consent issues related to that. But people understand that there is a big debate right now regarding making medical data more accessible for various critical social needs. Stan, would you like to start us off to highlight some of the major issues in that debate?

MR. CROSLEY: Sure. I think one of the major issues is consent. Beyond consent, I think you start with the traditional analysis that you've heard here in a couple of places, and that is, what's the utility to the individual, what's the benefit to the individual, what's the benefit to society? And society really not as a concept that's unknowable, but a society of patients who are dependent on discovery of medicines or other treatments. And then, what's the potential harm that can occur with the sharing of that information or with the actions that you want to undertake. I think it's really important to maintain that framework.

One of the issues that was raised here earlier is that we are on the cusp of -- and just the cusp, I mean, maybe the doorstep of the cusp -- of really

understanding personalized medicine. We are barely at the place where we are making medicines more safe. And we're able now because of either genetic sequencing or finding certain snips and probably morphisms that may identify certain illnesses or certain reactions to certain drugs, that we're administering them more safely. Due to genetic testing, certainly companion diagnostics is going to be become far more common over the next five years than you've seen so far. So, we are on the cusp of tailoring therapy now. And the first step is to make products more safe.

That said, the amount of information that exists in medical records, and even electronic records now -- we wouldn't have said that ten years ago -- but in electronic medical records is staggering. It's why the panels here are worried about the privacy issue, but it's also why the potential benefits are completely unknown. We can't even conceive of the benefits. And the worst possible step is to say that, well, we need to get a handle on medical research and slow it down because we want to make sure that we protect people's privacy. I think we need to make sure we protect against harm. I absolutely believe we need to prosecute harm mercilessly.

But I think that the transparency that's been talked about is important. I think consent is very

difficult in the medical records research space. Medical records as distinguished from interventional research, I think you're going to talk about that a little bit next. But medical records research data that already exists that is collected in traditional settings within the health care setting. Even a 3.2 percent opt-out rate, Art Kaplan at the University of Penn found, could completely bias the ability of a research effort to conclude a realizable result. So, you'll have bias because they found that the people who opt out have shared issues. So, by having those shared issues, you completely bias the research result. That's a safety issue. That's a life issue. People die when information isn't shared appropriately, and that is not a dramatic overstatement.

And so, it is critically important within research both from a safety perspective, a bio-surveillance perspective, and now as we step into pharmaco-genetic or genetic research, epidemiological research and pharmaco-epidemiological research, we need to kind of string together genetic information, medical records information, epidemiology to understand whether it's an underlying environmental or a genetic or a drug issue. So, the only way we're going to advance this medicine is to look at these issues that have been

identified on the panel. But I think that with research and within the traditional health care setting, there's a far more fundamental issue at hand and that is consent has an ethic that cuts both ways.

If we are saying you have to control your information and know how it's going to be used, and if you say yes or no, then that controls everything else that follows. I think that's too much burden on an individual. We need a paradigm or a structure on accountable use. What is expected for the use and how is that going to be permissible by saying -- and if do you that, then this is the frame and the people who are worried about how their information may be used, you can address the harms that can evolve from that.

MR. MOHAPATRA: Deborah?

DR. PEEL: Well, I really disagree. I think the public is not in that place that they've agreed to give up their data for the greater good in the sense that you're talking about. In fact, we're seeing some of that right now with the kind of attacks that are going on for newborn blood spots. I don't know if you all know the situation in Texas. We worked very hard, Patient Privacy Rights did, with the Genetic Alliance and some great technology companies to try to get a consent process to be used rather than have the spots be destroyed.

And so, what happened in Texas was the newborn blood spot program somehow kept 5.4 million spots without clear authorization, and then they did use them in ways that turned out to be very disturbing to people for various kinds of research projects without consent. And we need the newborn blood spot programs. Research has already shown that families are much more willing to share their information when they know that they're going to be asked, the newborn blood spots in particular. There seems to a growing number of people out there that are terrified of research for, I think, completely unreasonable reasons. And we have to be able to address them and say, no, you're not going to be forced to do this, and we need to be able to enable the rest of us that want research to say, yes, I want to keep those blood spots because if my kid gets cancer when she is 18, we can compare the DNA at age 18 with the DNA from birth and that will lead to some of the kinds of personalized treatment that you're talking about.

But I'm very, very concerned that unless we return to the basis of research ethics, which is the autonomy of the individual and the individual's right to choose, we don't want to kill the goose that's laying the golden eggs.

Just one other thing in my field, again mental

health, 30 or 40 percent of the people are off the grid and there are no records for them. No records. So, I'm selfishly hoping that we can have a really trusted system so people who see therapists, who get treatment besides drugs, with complicated mental conditions so that we can actually know what the best treatments would be. And I know we'll never get it in my field unless there is truly a trusted consent system.

MR. MOHAPATRA: Kim, do you have some thoughts?

MS. GRAY: Yes, thank you. Well, I think it's very unfortunate, to say it mildly, that these blood spots in Texas were destroyed. I think it's important to note that there was a disconnect in that particular situation and that my understanding is that this was de-identified information. And I think where we really need to enhance things, other than necessarily through consent, is by enhancing public understanding of the difference -- of just the significant difference between de-identified information and identifiable information.

The Texas case illustrates that lack of understanding by the public of just what can be done with de-identified information. And as Stanley had pointed out, consent is not always an easy thing to do when we're talking about research, and if we need to have the public good be the final goal of research, then we need some

other alternatives. And maybe one good alternative is the use of de-identified information.

I work for a company that does handle an awful lot of de-identified information. We receive roughly 75 percent of the prescription information in the United States in de-identified form. What comes to us is not someone's prescription information that identifies a person. Pharmacies are not selling us protected health information. But, in fact, we receive de-identified information, and then we treat it in such a manner that we put controls around that to avoid any appearance of re-identification, and we extend those controls not just internally, but to external entities that might, for some reason, have reason to have that data.

With using de-identified data, we're actually able to help not just commercial entities, but non-profits, state and local government both, we work hand-in-hand with a lot of research institutions, big names that you'd recognize that are reputable institutions such as Harvard, Yale, MIT, Duke, UNC, Hopkins, and I could go on and on from there. We have shared information with the Federal Government at the GAO, FDA, DEA, CMS, and I could go on from there, too.

But I'm offering another solution to the consent concern which is, let's use more de-identified

information and let's use less patient identifiable information. It's patient protective to do so. It still enhances research and allows that free flow that others on the panel have also noted is so required. You have to have a free flow of information. We can't be stymieing research, we can't be stifling innovation, or we're missing all the goals of better quality, better outcomes and enhanced health care in the new regime.

MR. MOHAPATRA: I think de-identification is something that hopefully we're going to have time to address in regards to whether or not medical data or certain other types of data, such as genetic data, can truly be de-identified. But I just want to go back to -- I want to ask Marc actually, are there alternative approaches in the research space aside from individual consent such as the Ontario model or the recommendations I believe you worked on with the Institute of Medicine?

MR. BOUTIN: There are other models. And I want to stress the importance that there is no silver bullet to this. And I've said this earlier. Consent is part of the solution. It's not the entire solution. The IOM recommendation was, in essence, to expand the HIPAA protections to all information in certain areas. The Ontario model allows information to be provided to an entity that oversees how it's used for different research

purposes. I think there were different ways to address this, but really at the heart of this is stratifying the issues both in terms of benefit and risk and then applying the appropriate solution to that metric. And I think that's the discussion we have not had.

The challenges, again, people don't understand consent. As I said earlier, 75 percent of the population does not understand what consent means or how their information will be used after they give consent. We can certainly do a lot better in that space and we have to. And there are models that have been utilized that have done better, but we still have not solved that problem.

If you look at how health information is evolving, take, for example, the lack of awareness that the treatments that we receive, on average, work 60 percent of the time. Most people with chronic conditions do not know that. Forty percent of the time you're essentially taking a placebo. For many complex conditions, cancer, neurologic conditions, it may only work 10 percent of the time. Within our lifetimes, we're going to solve that problem and figure out how to tailor the medicine so that we know it will work or not work for you. But that's going to come from research that's going to be at a large scale that is different from the kind of research we've done in the past that's going to take a

new model.

And I can tell you from the perspective of people with chronic conditions, they want this research to take place. They're still concerned about their privacy and security. They're still concerned about consent. But when faced with a life with a complex chronic condition and knowing that your children and grandchildren may face the same plight, you want that research to take place.

So, how do we balance these competing options? Again, consent is part of it, but we need to look at how we stratify the risk, the benefit, and then apply the appropriate metrics both in terms of privacy and in terms of safety. And so, what that means is there are going to be different levels applied to different areas. And until we have that conversation as a society and figure out how to stratify that, we're going to continually be at the spot that consent is the only solution and that privacy continues to be a problem. And we continue to see people not seeking care out of fear and not get the solutions in terms of research that we all need.

MR. MOHAPATRA: Thank you. Jodi?

MS. DANIEL: Thank you. I agree that I think that a lot of the benefits we're going to see in the health care arena are going to come from leveraging data

that will now be made available, hopefully, and be more useful based on health information technology. The question is, how do you then protect that information? And we're struggling with this because one of our goals is not only to improve individual health and coordination of care, but improve population health.

One of the things I keep hearing that I think is really intriguing and that folks have experimented with is trying to keep the data close to the source. So that when an entity has a research question or a public health agency has a question about how a particular treatment is working or what's going on in a particular population, that they can send a query to the entities that are holding the data and get back responses without getting access to the individual data. And the FDA is doing this with their Sentinel program. There are other examples of this, as well.

But it's a really interesting model for using data, not having that bias, but also not having the information flowing all over the place. So, it's, I think, a really good model to look at and see how much we can leverage that to both protect the data, but also have the data that's necessary for research and get the results that the data can provide.

MR. MOHAPATRA: I have a question for Linda

related to the research space. I know that you had previously mentioned to us in our research calls the way that 23 and Me had operated in terms of protecting the data, but working with researchers to get results that they were interested in.

MS. AVEY: Yeah. Well, it's a model that is -- and it's sort of still theoretical, but the idea is that having massive amounts of genetic data combined with phenotypic information that's been collected and layered on top of the genetics, when you talk to a researcher and they hear about that, they get really excited and they'd say, well, I'd love to have access to the data. But when you really probe them on it and get a little bit more information, it's like would you really know what to do if you had access to the information? Would you know how to run the queries? Do you have a statistics background? Do you know the algorithms to run? And they stop short and say no.

And if you even talk to people at the Brode Institute up in Cambridge, if you really ask them how many people truly have access to the data to run those queries, it's a handful. So, it's a very specific set of skills that a very few number of people have the ability to provide to an institution. That's just the fact of the matter.

So, if you've got researchers who understand a disease really well, they not geneticists and they're not statisticians, but they come up with a really good query, then you can run that against the data and get the end result of that and then share that information back to them. And they're happy, they go off and they continue their research. But the data has stayed in this very safe environment. So, I personally believe that that's a very operable model.

And when the NIH came out with dbGap, which was this database where they were going to -- because it was ironic that the NIH was saying, well, we're going to come up with this very open access model where you're going to have access to all of these genotype data sets, and a group of individuals who were actually studying the forensics field were looking at whether if there is a pool of blood samples of multiple individuals that you could pluck out the DNA of one individual and they actually came up with a way to do that.

Well, the same is true in insilico (phonetic) data, that you can do the same thing, where if you pluck out a few bits of a person's profile, you can pull out their whole profile. And they pulled dbGap down for that reason because they realized there is no such thing as de-identified genetic data. So, it's worth looking at

these models that people are coming up with and we do believe that that is a very solid way to do it that protects people, but also enables research.

MS. GARRISON: And also, Kim, to go back to your earlier comments about the de-identified prescription data that you get, again the protections that you apply to it and the controls that you apply to it, none of this falls under HIPAA. It is what your company does as a practice. Can you talk also a little bit about what happens when you get queries to this -- to you for information about or access to the data? What are the controls that you want to place on that to the recipients and what, in some instances, are their responses?

MS. GRAY: First of all, much of what we do is actually in report form. We're not actually giving raw data. We're giving reports that summarize it because, of course, we are the ones that do the statistical analysis as opposed to the research, as was earlier pointed out.

In those occasions, however, when a researcher wants particular information from us, we do impose the same kinds of controls on them that we would with anyone else who would want that particular information. So, for example, whereas internally we have security around the folks who are working with this de-identified data, only

certain people have access to it, they're trained as to good practices around it, we extend those same requirements by contract to others. And we will occasionally get pushback from researchers who don't want to play in the same playing field that we're playing in. They don't get that information. That is a requirement. So, for those few researchers that don't want to play ball with us, we will not be sharing the information.

But I must say that most researchers are not looking for that anyway. They are looking for the aggregated information because they don't have the statistical ability and it's much more useful for them to have the aggregated data tables. And those controls would be onerous, in some cases, to put on individual researchers who are not necessarily affiliated with the larger institutions.

MS. GARRISON: Jamie, quickly.

MR. HEYWOOD: Well, we run similar systems to 23 and Me and I think IMS in that we sort of retain the data, we run the queries, we'll ask the questions. And we've struggled with this question because I think we have a trust relationship with our consumers. And we impose that same trust restrictions which are non-re-identification and discrimination on our partners.

But, actually, I'm really uncomfortable with

the use of the word “de-identified.” I think it’s -- I mean, I will tell you that if you look at the 10,000 of our patients that are public, you could, with 100 percent accuracy, pattern match them to your system, and there’s no question that that’s possible, and it’s a query that you could run on patients that are putting public information to profile.

So, I think that we should -- we have to be honest about this question. If you have four data points about a patient, I mean, even the implication that a genomic spot that you know, the date of birth and the gender and the city, that that’s de-identified? I mean, there’s no more specific identifiable subdata in the world. So, under those conditions, I think we really are talking about this question of a trust framework not a de-identification type framework. And I certainly would not pretend to our customers that the information is de-identifiable. In fact, we explicitly say that it can be re-identified on the website in three FAQs. So, it’s very -- this is a very -- I think it’s a very, very dangerous term that we should not use at all anymore.

MS. GARRISON: Okay. What I’d like to do is to give each panelist about a minute to reflect back on all the issues we’ve discussed today and just present two or three key points that you think are most important.

We'll start at the far end with Marc.

MR. BOUTIN: I'll just conclude by saying that we have a long history of protecting privacy. We also have a long history of promoting public good and social interests. And there's been a balance between those two competing aims historically. The balance ebbs and flows depending on the context of where we are as a society. And I think we're at one of those critical points in time where society is changing. Technology is changing. Information is changing. Health and the way we deliver health and the way we develop treatments are all changing. So, we're at a pivotal point in our time. So, it makes sense that we're having this conversation.

I think the challenge is to, again, get the balance right for our current needs and realize that it is not a zero sum game. Privacy is not going to totally trump social need. Social need or social good is not going to totally trump privacy. The challenge is to get the right balance, given our opportunity, both at the individual level and at the societal level. So, I thank you for taking the time to listen to me.

MS. GARRISON: Kim?

MS. GRAY: Two points. First of all, to the de-identification point, I'm not going to disagree with Jamie that things can be re-identified. However, I think

Jamie makes an important point in that he notes that these are publicly available points. His work is done via a public vehicle. And I think as long as we are not -- and any previous re-identification that's been published has all been because of publicly available information.

I think the important thing to do is to ensure that your controls, if you're working with de-identified information, are not just your internal policies and procedures and your oversight, having your privacy officer at your company and your security safeguards, but that further step of restricting anyone downstream from re-identification, and if there is re-identification, have penalties for it. CMPs or whatever it happens to be, that if somebody is going to go that extra step, by commingling with publicly available data and doing a re-identification, they should suffer the consequences for that and then internally continue to reassess your processes to make sure you're keeping pace with technology and that you're not allowing that same thing to happen, which is my segue into point two, which is be accountable.

IMS is not a covered entity. We are doing things that we've chosen to do because we are an accountable organization and we do care about patient

privacy and we also care about research and all the other public good that's coming from it. Accountable organizations take this organizational commitment from the top. They put their internal policies and procedures in place. They have privacy protection goals that consider many things, laws, public policy, best practices, and self-regulation as a part of that. They do training and education. They believe in transparency. They demonstrate that they can do what they say they're doing, public education about what they're doing. And then, lastly, mitigating any harms, if there should be one that occurs, and taking their lumps as a final step being enforcement.

And this accountability principal is one that's not new and it's global and I think we need to think globally because privacy is global. Many of us are in global companies. But bottom line is privacy is global and the accountability principles started with OECD, the EU has it, PIPEDA and Canada have it, APEC has it. And even Gramm-Leach-Bliley, to some extent, has it because it all says, here's the end where we want to get. Our means may differ as to how we get there, but back to that whole trust thing that's permeated this panel discussion today, if we have accountable organizations that go down this pathway, we've got the trust that's needed by

consumers.

MS. GARRISON: Thank you. Deven?

MS. McGRAW: We absolutely have to make sure that personal health information is protected wherever it is. And we have some protections for it whether it's in the health care system and we don't have them when it leaks out or is voluntarily put up by consumers. So, at a minimum, we can count on accountable organizations to some degree, but there are a lot of organizations that are taking advantage of a rule-free environment and they're, quite frankly, going to spoil -- upset the apple cart for those who are accountable.

So, at a minimum, some baseline rules that apply, consent should play a much bigger role because this is a consumer-based world and, to some extent, what they would want to do with their data, they ought to be able to do with their data. We need to be much more clear about telling them what the risks are, not just buried in privacy policies, but through other techniques and devices that can get consent in a more clear and obvious way.

But we can't just count, in fact, on consent. As many people have said very well today, it's an imperfect protector of privacy. Nice alliteration there. So, as a result, we also need to look at what might be

patently unfair to consumers that's going on out there, for which the FTC actually already has jurisdiction to crack down on.

MS. GARRISON: Jamie?

MR. HEYWOOD: This is, to my mind, a much bigger question than privacy. I think that we stand at a moment in time where the sort of very fabric of our modern society is being challenged by technologies that are connecting us in new ways. And I think that the choice that we have to ask ourselves now is, how do we approach this problem? While many of the technical details of this, I think I agree and we could disagree with, but I think there's a principle that I want to elevate up one level which is, what kind of world do we want to live in? Do we want to live in a world that is transparent, that is open, that is collaborative, that is honest, or do we want to live in a world where we are preventing the flow of the blood of humanity, which is information, because we are so weak, we have chosen not to address discrimination?

And I think this choice now is between a hard and an easy road. And the easy road is to say, oh, discrimination is bad, let's make sure that anyone that makes any information flow anywhere that makes discrimination happen is punished, because it's easy to

punish people that deal in information. The hard road is to actually live to the principle that all are created equal and incorporate it in law and make discrimination not happen. So, if the consequences go away, of the flow of information goes away, so the stigma, which is the problem we're talking about, goes away because people come into light with issues and that we collaboratively solve problems as a society. And I think we don't face this choice well. We're making the decision to look at information and not discrimination, and I think we should really look and ask ourselves what world do we want to live in as we develop these policies?

MS. GARRISON: Thank you. We are the only ones standing between this group and lunch, so Deborah?

DR. PEEL: I'll try to go quickly. Yeah, I appreciate what you're saying about the wider question and what kind of world do we live in. And I think most Americans want to live in a democracy and the fundamental, most important, personal liberties and personal rights have to do with being able to be separate and not have everything be known about you. I think in the words of Supreme Court Justice Brandies, I think he said, the highest right of civilized man is the right to be let alone, the right to have privacy is essential to democracy.

And I really appreciate -- I think that actually there's a lot of agreement on the panel that the ability to consent is very important and that individuals should make choices. But I would just like to point out that consent is not in the meaningful use criteria for all of the EHRs that are going to be purchased to start this connected world. We don't have the ability to control this information currently. And so, that's a really important point. And since this panel does agree that some degree of consent is needed, maybe you can help us work with the agencies and make sure that gets in there.

I know our coalition wrote a letter and asked the Health IT Policy Committee to be sure and put consumer controls in up-front and they're not. They're at the very back. So, that's really important to understand. And then, in terms of things like trusted organizations, at some point we're going to need an external trusted consumer organization that can evaluate the claims of all of these companies, whether they really do what they say or not because it really is impossible for individuals to figure it out.

So, individuals have rights. And as you think about this, I hope you'll think about who you think can make the best decisions for you and your family about

your sensitive health information.

MS. GARRISON; Thank you. Jodi?

MS. DANIEL: Thank you. I believe that we need a privacy and security framework that applies to all entities that hold information and that we need to do a better job of preventing and addressing harm, as Jamie had mentioned. I think we need to do both.

I think the fact that we have uneven protections is a problem because it affects trust. So, if a patient assumes that information is protected because there is some law in this space, the HIPAA laws, and don't understand that it might not be protected in another environment and that information is used in a way that they didn't anticipate, it erodes trust. And I think if we don't have this framework, we're not going to realize all of the benefits that we can realize, both from consumer engagement, from having better information to help support research, et cetera.

We're doing a couple things I wanted to quickly mention. We do have a privacy and security framework for health information exchange at HHS that ONC released in December of 2008 which tries to focus on fair information practices, including consumer choice and transparency. We're working on a model, an online privacy notice that folks could use to help improve transparency as to how

information is being used. And we're also looking at how to protect information held by non-covered entities. This is something that Congress required to us to do under the high-tech act. And we're also looking at consumer choice policies through our privacy and security policy committee, et cetera.

The issue here is that all of these things we're doing are voluntary. I mean, we're not talking about a government mandate to protect information in these certain ways. And I think we do need to think about how we hold people accountable and make sure that there is an even framework so that there are not some actors who are trying to do the right thing and others that are blatantly using information in ways that folks would not understand or anticipate and not communicating that to folks. So, that's it.

MS. GARRISON: Thank you. Linda?

MS. AVEY: So, I agree with everything everyone else is saying. One of the things that I think would be really interesting to look at is, could the government be in a position to really point out success stories? Were have we seen companies that have done a really good job, who have shared information and enabled consumers to get their information out and where it's been used productively? Because I think we talk in theoreticals

when we talk about all of these harms and the scary stuff.

When somebody loses a computer with a database on it, that's the story? You know, what happened? What was the implication from that? What was the result of a computer with information on it being lost? We don't ever really challenge these fears that people have. They're just sort of unknowing, but they think that sounds scary and I think that's why they answer surveys and they say, oh, I would never want my information out there. But nobody ever challenges them on that.

But, instead, if we can turn this whole thing around and say, here's the situation where people shared information and here's a really positive outcome that came from that and let's reward that behavior. And then certainly, as Stan was saying, if we know places where people are not following what they say they're going to do and they don't abide by their own self-imposed rules or others, that they are prosecuted.

So, we have laws in place that allow us to do that and I think the government has things to challenge companies that are the bad actors, but let's not put everybody in the same bucket, and really reward success if we can.

MS. GARRISON; It's much easier to challenge

when you have standards.

MS. AVEY: Exactly.

MS. GARRISON: Stan.

MR. CROSLEY: I'm stuck here with the traditional and non-traditional concepts, as well. And I think within the traditional concepts, there are easier solutions for research and things where we look at public benefit and we see a societal benefit and improvement to individual's health care and quality. I think uses can be better understood and I think we can move to models, like Linda suggested, models that, in fact, Ontario has with trusted entities or even the FCRA, they have a trusted entity concept on access and utilization of information. Not everybody gets access to the information. So, I think those are models that are valid. I think the OIM report talked about some of those.

The non-traditional setting is much tougher. It's much more difficult. And I think Jamie set out the concept of how transparency is just ultimately so critical. And I couldn't agree more with that. I also believe that the table stakes, regardless of whether it's traditional or non-traditional, is security. I mean, I don't think there's any excuse whatsoever for not having appropriate security around health information. I don't

care where it is or who has it. I would be in favor of understanding how some type of a framework could address the security issues.

Control is a much different and much more difficult concept. And I think we need to keep working our way through it.

MS. GARRISON: Terrific. I want to thank each and every one of our panelists for a very stimulating conversation. Thank you.

(Applause)

(Panel 2 was concluded.)

PANEL 3: ADDRESSING SENSITIVE INFORMATION

MS. HARRINGTON-MCBRIDE: Good afternoon, everyone, and welcome back from lunch. For those of you in the building, I'm glad to see you back in your seats. For everyone on the webcast, welcome as well.

My name is Katie Harrington-McBride. I'm a staff attorney with the FTC. Together with my colleague, Michelle Rosenthal, we will be moderating this afternoon's panel exploring the treatment of sensitive information. Just a quick reminder, we will be accepting audience questions. If you're live in the room and would like to raise your hand with one of the question cards, one of our folks will come around and collect that and provide it to us. If you are out in webcast land, feel free to send an e-mail to privacyroundtable@FTC.gov.

In this morning's panel on health privacy issue, the question of sensitivity of health data, however that term might ultimately be defined, was at issue. This afternoon, we'll take an even broader look at what constitutes sensitive information for privacy purposes. We'll examine the core characteristics that make data sensitive. We'll look at some of the challenges to defining sensitive information, and we'll discuss whether such data should be subject to particular restrictions, for example, collection, use, sharing or

disposal restrictions.

I know that the first panel after lunch is often a difficult one for those of you who may have carb-loaded, as some of us did in the green room. So, for context clues, let me let you know that we're going to split this into basically two halves. The first half of the discussion will focus on definitional issues and challenges and the second half will look at potential remedies for some of the problems we may be able to suss out.

We feel compelled, Michelle and I, to let you know that our sartorial sameness was not intentional and we also both apologize for not wearing kelly green, and we thank those of you in the audience who are wearing green today.

I'm delighted to welcome our excellent panelists who will help us sort out these issues today, and I'll briefly introduce them before we begin. To my left, we have Parry Aftab who heads WiredSafety and WiredTrust. Next is Anita Allen, a professor at the University of Pennsylvania. Next to Anita, Pam Dixon, Executive Director of the World Privacy Forum. Next, Jim Harper, Director of Information Policy Studies at The Cato Institute. Next to Jim, we have Kathryn Montgomery, a professor at the American University School of

Communication. Next to Katherine, we have Lee Peeler, President of the National Advertising Review Council, Council of Better Business Bureaus. And, finally, last but not least, we have Lior Strahilevitz from the University of Chicago School of Law.

We are so grateful to each of you panelists for coming to talk about this difficult issue. It's not only difficult, but it is amorphous. So, we have our work cut out for us.

In our calls with our panelists, you all will recall -- and I'm cluing you all in since you weren't on the call. In our calls with many other experts that we interviewed in preparation for this and even in our research, we learned that achieving consensus about how one might go about categorizing data as sensitive is maybe a tall order for a 90-minute panel.

When you factor in the diversity of opinions about how you might bound a definition of each of these types of data -- well, you remember the challenge of doing that in just one context, health information this morning. So, our goal today is really to focus on the characteristics that make data sensitive. To talk about extracting the rule, about what is it really at its core that makes something sensitive, to talk about those things. And, in particular, in our conversations with

panelists, what we've learned is that mostly what it seems to come down to is the propensity of certain information to cause particular harm. So, we wanted to focus the first part of our discussion today on some of those harms and we thought we would start with the propensity of information to cause physical harm.

So, physical harm is a concrete and cognizable form of harm. We all know this. This is intuitive and obvious. If data, such as location information, can be used to subject a person to physical harm, should it be considered sensitive? And to start, why don't we go to Parry?

MS. AFTAB: Thank you. If somebody can find you, they may find you in real life. So, as we start looking at these issues, at WiredSafety, we deal with cyber-stalking, cyber-harassment and cyber-bullying. So, if someone knows where you are, they may show up at your door. We've seen a lot of situations where kids have been targeting someone who is black onto a white supremacist website, harassing them in the name of a black student saying, if you don't like it, this is where you find me, name, address and telephone number, and people show up at their door.

We're also seeing some cases of breaking and entering, where someone will show up at your house when

you have tweeted about this great vacation you're going on for three weeks. So, where you are and how various devices and where sharing that information can be used to hurt us is something we're just starting to learn.

MS. HARRINGTON-McBRIDE: Any other thoughts about that, Jim?

MR. HARPER: Well, sure. I think personal security is an important privacy value, if you will, something that may not be in your best definition of privacy, an aspect of privacy. But I don't think you can follow the train of logic that information that could be used to physically harm you is sensitive information. Think about how that explodes things if you just take some of the notable examples, like the murder of Rebecca Shaeffer, for example, which used address information. Are we going to make address information sensitive information subject to special controls when address information is constantly shared with all kinds of parties for lots of good reasons? It just sort of explodes sensitivity to go that direction.

Obviously, personal security is an essential value. Harms to personal security are serious harms that need to be reckoned with. But it doesn't follow from that that data that could be used to harm you is sensitive.

MS. HARRINGTON-McBRIDE: Lior, the question about whether public information, that is something like address that is widely publicized, can be sensitive. That might be one that I would pose to you. Is that something that we should -- if we're going to look at this as a harms-based model. Can we cast the net as broadly as address or are we going too far there?

MR. STRAHILEVITZ: Well, with address, I think it is somewhat complicated in that individuals can elect to have a listed or unlisted address. So, there may be a consent model that works reasonably well, even with the old-fashioned white pages which I guess nobody uses anymore, although there remain white page analogs online that people are presumably using.

On the broader question, though, I do think that in terms of figuring out what information is sensitive, that Jim's right. Privacy may be, in 99 percent of all cases, a necessary aspect to the definition of sensitivity. In other words, it's very hard to come up with cases in which information is public, whatever the meaning of public is, some people would like that meaning to be broad; some people would like it to be narrow within privacy law. The meaning of what's private looks very different in, say, the privacy act versus FOIA's privacy provisions versus, say, New

York tort law.

But I think as a general rule, if we're trying to think of clear principles that might help us inform this debate, if it's truly private, then it may be sensitive. If it is public, it's very hard to construct a theory as to why it's sensitive. It's very hard to construct a theory, I think, as to why it's harmful if disclosed. So, HIV status, from the last panel we know, is almost always extremely sensitive, it's extremely damaging if disclosed. But to disclose Magic Johnson's HIV status no longer is harmful to him. You might describe that information as no longer sensitive and, indeed, for some of the reasons I think Jim was alluding to, there would, of course, be significant First Amendment constraints on any efforts to clamp down on discussions of the HIV positive status of someone who is well known for being HIV positive.

John Edwards' extramarital affairs, right? We can come up with a number of examples in which the information is so widely known by the public, that even though the subject matter makes us think it's sensitive, the scope of the disclosure means it no longer ought to be so, at least for these public figures.

MS. HARRINGTON-McBRIDE: Jim?

MR. HARPER: I would just add that even outside

the realm of public figures, there are people, there are communities who broadcast their HIV status through tattoos and things like that. There are many, many subcultures in our society that treat information that could be highly personal, highly private to some as public to others. So, it's really, really subjective, and that's the problem with broad definitions.

MS. HARRINGTON-McBRIDE: An excellent segue. Subjectivity is obviously at issue here and it comes down to, I guess, the difficulty of figuring out when a particular individual might have a subjective desire to safeguard some information.

Kathryn, could you speak a little about this in the context of your work, particularly with children?

MS. MONTGOMERY: Yeah. First of all, you know, this notion of defining sensitive information, only on the basis of harms, makes me a little uncomfortable. I think it sets up a certain high level of expectation there and I think we may be able to talk about kinds of information that we all agree are sensitive without being able necessarily to identify harms. I think it also may have to do with what you, as an individual, choose to disclose, as you were saying.

So, I think we may want to sort of talk a little bit about that. But I was involved in the 1990s

with the FTC and with Congress in passing the Children's Online Privacy Protection Act. That law acknowledged that children are sensitive -- what I would call sensitive users, and that is -- that law applies only to children under the age of 13, too, by the way. But that the information that they disclose and the information that is collected on them is, by definition, according to law, sensitive information. And I think that continues to be an issue.

I've been looking recently at the role of adolescents in the new media environment. And I think particularly when you look at social networks and the kinds of information that they voluntarily disclose, as well as what is gathered on teens, at an age when many of them are not necessarily turning, at the age of 13, into the wisest young people -- it depends upon the kid, obviously -- they can sometimes put themselves in harm in many ways and there have certainly been examples of that.

MS. HARRINGTON-McBRIDE: Pam, in the context of one particular group, victims of domestic violence, how does this play out? I mean, obviously, there's a very real risk of physical harm in that case, even from the release of information that might, by other people, be considered very public, address information, but which a

victim of domestic violence might be striving very hard to safeguard. How would we have to treat something like that, that very particular instance?

MS. DIXON: Right. It's a good question. I think one of the things that's pointed out by the conversation so far is that the issue of sensitive information is an issue dealing with borders and borderlines and how incredibly difficult the borderlines are here.

So, let's start with public information. So, you have a victim of domestic violence who, prior to the relationship that was problematic, published their address information and other locational information without fear of any consequence. So, they, themselves, made it public or allowed it to become public for whatever reason. And then after, you know, a difficult situation, then their situation changed. So, now you have information that's in the public realm and information that can, in fact, potentially harm that person. Or let's say they've gone to great lengths to then move or somehow change their status, so that now the new location information or address information is now private. That information now is sensitive to them.

So, what do you do in that case? You have public information for some people and private for

another. This leads to what Kathryn was saying about sensitive users. I think that it's fair to cordon off some categories of individuals as sensitive users. I would also suggest that individuals who have various kinds of challenges that would, for example, diminish their ability to consent or to make meaningful decisions about what constitutes sensitive information, that would be a challenge, so the very elderly, individuals with mental challenges, et cetera.

But something worth thinking about further here is the borderlines, and you can really see this in health information as well. So, an individual has a health condition for which they need to borrow money to pay. Let's say it's an HIV/AIDS status or even a cancer treatment. They need to borrow $10,000 for treatment. They go to the bank and they get a loan for this medical treatment. So, here's the question. Is that medical data? Is that bank data? What laws apply here and what protections would apply in terms of data sensitivity? Because this is -- as soon as you try to say that, for example, medical data, or, you know, victims of domestic violence data is sensitive, all of a sudden it gets very messy because it all starts to spill over the borders.

So, then you arrive at a position of, well, does the protection travel with the data? And then that

helps you through the border issue, unless you have a victims of domestic violence situation where your status could change.

So, what I'm saying is that this is a very complex, very messy issue, and I don't think there are any easy answers here. I think that because of our sectoral system, we have quite a pickle in trying to solve it.

MS. HARRINGTON-McBRIDE: I think fair enough. And, yet, we still have the good hour and 40 minutes left. So, we're going to keep at it. Don't anybody get up and go now.

(Laughter.)

MS. HARRINGTON-McBRIDE: Please don't move your chairs. But Pam is right. I mean, I've got to tell you, we've been in deep on this now for six weeks, Michelle and I, talking with these panelists, who have been extremely generous with their time, and a variety of other experts. Some of whom are in the room. And it really is -- I mean, it's Alice in Wonderland. You're down one rabbit hole and then you're into the next.

I want to go back to the location issue. We moved very quickly from location to address. Of course, address is very public and widely known. In our second privacy roundtable at Berkeley last month, or I guess now

it’s a month and a half ago, we talked about the issue of location tracking. And that’s different than address. That’s where I am now. This is not my address, but it happens to be where I am. I’ll be someplace else tonight -- hopefully, all of you will be, too -- celebrating St. Patrick’s Day. That information is different, isn’t it?

So, Anita, tell us about your thoughts about the sensitivity of that information, vis-a-vis, individuals who may or may not have any subjective issues with their privacy, but how does that play out, and not only their specific location but location tracking over time? What are the concerns there?

MS. ALLEN: Well, one striking thing about your question is that I think if you ask the average person on the street, what are the major categories of sensitive information, they wouldn’t say locational first. They’d say, oh, medical, financial, educational, sexual. They might even say sexual orientation information and they might even say race and ethnicity information. But locational information is sort of a new way to think about a kind of information which we might regard as sensitive.

And one area in which locational information becomes very important in the area of criminal justice, criminal procedure. Oftentimes, we don’t want people to

know exactly where we are because we're doing something we shouldn't be doing. And public policymakers may want to fight public policies that make it harder for law enforcement, national security to get access to location precisely because it's the bad people who are going to care the most about others not knowing where they are.

Yet, all of us, no matter what we're doing, whether we're baking cookies or, you know, making crack cocaine we don't necessarily want the world to know exactly where we are at a given moment. We might be having a secret rendezvous. Again, we might just be making cookies. So, I do think there's something to the idea that we need to treat locational data as a category of sensitive information. Not perhaps as sensitive as a person's medical records, but pretty importantly protected.

MS. HARRINGTON-McBRIDE: Lee, do you have any thoughts about the tracking of location data over time, not just where I am now, but the amalgamation of a pattern of movement for an individual and whether that poses challenges or should be treated differently than individual points where a person might be at any given time?

MR. PEELER: Yes, I do. And it also seems like just -- you know, the framework of what we're trying to

do here is talk about where information is more sensitive than ordinary information. And, you know, as you said, it's very contextually driven. And, you know, this type of discussion that the FTC is leading, I think, is extremely valuable in looking at sort of evolving issues like location information and trying to basically analogize them to what we've done in the past.

I thought Kathryn made a really good point that one of the first areas that we've looked at, a while ago actually, was kids' information, and there were really two issues that drove that. One was risk of harm, which is what we're focusing on now. But the other important issue in the kids' area was the feeling that young children just couldn't appreciate the trade-off that was involved or the risk that was involved in disclosing personally identifiable information over the Internet. So, you had those two factors coming together to establish a higher level of protection.

And I think, you know, if you're analyzing location information, you have to follow sort of that same approach, all information should be accorded fair information handling practices. There are lots of people out there that make their location information known, you know, widely. It's on Facebook and people tweet where they are and where they're going and things like that.

So, establishing sort of a broad category that says all location information is sensitive, I think it's likely a step too far.

MS. HARRINGTON-McBRIDE: I think you've raised some really interesting points. I'm going to come back to you, Kathryn, really quickly here. But when you mention this sort of two-part analysis, that there's both a risk of harm and an inability on the part of the individual to meaningfully consent, either they're under the age of consent deemed by law or there is some other factor that prevents them maybe from being a full participant in this transaction. Maybe we should go to the example of the prevalence of self-provided data in location tracking. We all know that many people do it. Lee has annunciated this principle and we all know it from our friends. We see where they are and where they've checked in and what they're the mayor of. That information, though, that's self-provided.

So, by one argument, maybe Lior would say, you know, you've made that public and told everybody where you are and that's your choice and you're broadcasting that. One question that might come about is what about secondary uses? So, many of you may have seen in the media recently the pleaserobme.com website went up and it aggregated location information from foursquare and

Twitter and other places where people willingly provide their location. The idea of the website was to say, well, these people are not at home, so if anybody would like to pop by and maybe grab a new TV, now is the time.

So, the question becomes really, what about secondary uses of this information? Even where information is self-provided, is there a deep enough understanding on the part of the populous using tools like this about the potential risks for either amalgamation of that data with something else or just repurposing of it?

Kathryn, I wanted to get to you, too.

MS. MONTGOMERY: One thing I wanted to comment on because thinking back to COPPA is like thinking back to ancient history when I remember the research we did on kids and the fact that they were being asked questions and filling out a questionnaire and volunteering the information, and while a lot of that still happens in the digital media, a lot of what we're talking about here -- and I'm glad you raised this broader issue -- is more behavioral targeting and behavioral profiling and data collection that's happening in a much more automated and passive way where we're not thinking I'm going to volunteer this information about where I am.

So, for example, with mobile marketing, the

whole growth of location-based targeting is based on the fact that these technologies are capable of tracking where we are. So, we're not really thinking so much about every instance of what we're doing. Nor do most consumers, I would argue, fully understand the extent of data collection and behavioral targeting in today's contemporary digital marketing environment.

The other thing is that talking about sensitive information in discreet terms, I think, obscures the fact that -- another issue you raised -- that it's really the ability of these technologies and these applications, and the marketing practices to amalgamate, to bring together, to converge all of this information, some of which you may have volunteered consciously, much of which you didn't, and to packets of information about you and profiles on you, that you have really no idea has happened.

MS. HARRINGTON-McBRIDE: Okay. Pam?

MS. DIXON: I'd like to kind of add on to -- accrete on to what Kathryn was saying. If you take, for example, the idea of a person who has their mobile phone on at a physician's office, that location information can easily be used in other ways. Something that certainly comes to mind is some of the digital signage issues. So, for example, just a few weeks ago, I ran into a digital

signage vendor that has a digital concierge product that once you interact with it with your mobile phone, if Bluetooth is on, then they get your Mac address and then they target ads to you based on that information. This is all done with kind of a passive consent because you have Bluetooth on, right?

So, this information, taken by itself, may not cause harm. But if you accrete this information over time and layer it with other bits of data, does this information become sensitive if this information is, for example, tied to a physician visit, or something that could be construed as sensitive? So, the whole idea of sensitive data in what context and sensitive data or little bits of data that become sensitive when combined with others, I think, is a very difficult and challenging concept, but one that we really do need to grapple with because I think it's very tempting to look at data as individual units or pieces. But that's really not how most folks work with data anymore. Most people have really nice computers and really nice systems that can crunch and munch a lot of data, and I think we need to think about that context as well.

MS. HARRINGTON-McBRIDE: It's a Monet and we need to stop looking at brush strokes is what you're telling us?

MS. DIXON: Absolutely.

MS. HARRINGTON-McBRIDE: Parry?

MS. AFTAB: I'll address your question.

MS. HARRINGTON-McBRIDE: Thank you.

MS. AFTAB: Whenever I'm asked about sensitive information, I break them into two pieces. One is kids, cash and kidneys; children, financial and health. And in the United States, that's where we tend to regulate. Those are the things we care about, whereas in Europe, they care about trade unions and a lot of things that in the United States we don't consider sensitive.

I also identify vulnerable groups or vulnerable users, those who are more likely to be targeted because of who they are, whether it's sexual preference or racial background or ethnicity or age or you're the victim of crime, those kinds of things, who are more vulnerable. Once you get into a vulnerable group and it touches data that otherwise might not be deemed sensitive, like King Midas, it turns it to gold.

So, when you take location information, that might not be a problem if it's in the White Pages or Yellow Pages or the kind of thing that you can look up. But you're now dealing with a victim of violence and she's trying to hide where she is or hide the kids, it now becomes sensitive. So, how do we, in secondary

usage, know that information that we might not have considered sensitive is now made sensitive because it involves a vulnerable group member. And that's part of the problem.

I think as we start to look at this we need to create higher burdens on the people who are going to use it for secondary use. I think this is the FTC. I think that commercial use is something we can do a lot more about than we can individuals who are saying a lot of hateful things that may be covered by the First Amendment whereas commercial speech may not be. So, I think that as we're looking at secondary uses and date miners and profiling and a lot of those things that are happening, all you have to do is look at the front page of today's New York Times and see how little bits of information become a big mass of information.

I think that we need to turn around and say to somebody, for commercial uses, you need to know where it came from and you have to be responsible for it. You can tie it to -- you can tag it using electronics -- and I know we'll talk about this in the second half, but there are a lot of different things you can do. But I think we need to turn around and say, if you want to use it for commercial purposes, you're going to start to combine it with something else, you have to know where it came from.

So, it has to have some type of authenticity, some type of verification. Otherwise, it's hands off.

MS. HARRINGTON-McBRIDE: Okay. Anita and Jim briefly, and then I think we're going to move on to our next type of harm.

MS. ALLEN: Yes, briefly, I totally agree with Parry and just wanted to add that you do have -- this question of intersection, what happens when you intersect the vulnerable groups with the information which is either inherently sensitive, or we might say it's inherently sensitive, and the information which is not really all that sensitive, but when combined with a vulnerable group it becomes something we want to call sensitive. So, I totally agree with that point, that we have to think about the intersections of all these bits of data.

But I also want to emphasize that it's not just the question of what do individual people who might be thieves do with my locational data and what do commercial actors do with my personal data? But I want to go back to the government, also, because the government has access to our Amtrak travel records and our airline travel records. All that locational data, all that data which when aggregated provides a portrait of our lives, it's in the hands of somebody, not just commercial

sector, but also the government.

MS. HARRINGTON-McBRIDE: Jim?

MR. HARPER: Well, I think we run into problems defining sensitive data. There's more likely to be some traction in defining sensitive persons or groups. But I'll throw some complexity into that. As a website operator myself -- everybody should be one.

(Laughter.)

MR. HARPER: I have comments on a site that I run called WashingtonWatch.com that run into hundreds per day, easily. One bill in particular has 114,000 comments on it right now. And there's no way to manage that comment system other than trying to just automatically induce people to stop swearing so much. But I don't know in advance who a person is that's commenting on there. It is a very open -- it's a wide open system. Anybody can comment without identifying themselves. I don't know in advance who they are, what category they're in. I don't know whether they're telling the truth or not when they say who they are or when they say things about themselves.

I've seen even today someone say something about herself, about a domestic violence situation she's in that would be very stupid to say if you were in one. But I have no way to adjudicate whether that's true or

not. I have no way to adjudicate whether she's even a woman.

MS. HARRINGTON-McBRIDE: And we're going to talk about some of those real challenges to businesses of implementation of any of the kinds of cures that we might propose. But to get back to the identification maybe of the harms, we've talked about two other kinds on our calls, two primary types. One being financial harm that can occur, and I think that that one is a little more concrete and tangible than the other kind, and that is, dignitary or social harms, the idea that some data is sensitive because we simply don't want other people, or at least not broad swaths of people, to know about it.

So, let's talk about those maybe in contrast to one another. Cognizable claims under law for both kinds of harms as we know. But when it gets down to this data may cause someone embarrassment or anxiety or social distress, is there something that should be done about that? Should a system of regulation account for that somehow or is it simply too difficult to get your hands around in any sort of regulatory scheme? How would you deal with that, Lior?

MR. STRAHILEVITZ: Well, I think one of the common misconceptions about the work that people who legislate or regulate or hand down case law in

information privacy cases is that the harms from disclosure are one-sided. And I actually think a sophisticated understanding of how privacy law works and what privacy law does suggests that with respect to financial harms, dignitary harms, there are often harms on both sides.

So, let me provide one example to see if I can make that more concrete. I think this would fall under the stigmatization harm or the emotional distress harm. Let's think about criminal history information. There's been a huge move in nearly 50 states to publish information about crimes that individuals have committed. We know, because it's most prominent, about the sex offense registries. But California is now considering legislation with respect to animal rights abusers registries, arson registries are already on the books, burglary registries in some states. So, what should the law do with respect to these sorts of issues?

Well, there's obviously a harm to the ex-offender whose information is disclosed and who's trying to reintegrate themselves into society, and that seems clear. What I think is less obvious, though, but equally important -- and this is part of what makes these sorts of issues so difficult -- is that not disclosing information harms other people, right?

So, with respect to criminal history information, there's very disturbing, but actually extremely well done technically, research that Harry Holzer, who's here at Georgetown, has done along with Michael Stoll and Steven Raphael. And they looked at the labor market consequences of criminal history disclosures and found that in those jurisdictions where criminal history information is made most transparent, the employment outcomes of African-American males in, let's say, blue collar entry level positions do better. In other words, in the absence of reliable criminal history information, employers for blue collar positions tend to assume that roughly all African-American males have criminal histories and then, as a result, refuse to hire them, regardless of whether they've got a criminal record or not.

So, that's an instance in which, because of existing biases, because of discriminatory behavior, you're sort of caught between a rock and a hard place, right? If you're interested in advancing the cause of racial justice, if you're interested in undermining this propensity of employers to punish African-American males, refuse to hire them simply because African-American males as a whole have a higher propensity to have criminal convictions, then you might want a system of no privacy

or what people in this room might refer to as no privacy, which is complete transparency with respect to criminal history information.

By the same token, though, if you focus on the marginalized population, the ex-offenders themselves and you look at the effects of the Megan's Law registries, other registries that try to create greater transparency for criminal history, you'll say, well, there's an obvious harm to them if this information is publicized.

So, I guess what I want to suggest by way of this is that while it's very useful to talk about sensitivity, it's very useful to talk about the propensity for harm and both financial harms and other dignitary and stigmatization harms, ultimately what the FTC is going to have to do and what lawmakers are going to have to do, is confront these wrenching trade-offs because privacy law inevitably creates some winners and some losers and the government simply has to decide, in these cases, who the winners or losers should be.

MS. HARRINGTON-McBRIDE: So that I don't take time away from the very important work that Michelle is going to do in just a few minutes, we're going to skip lightly over a couple of topics that we've actually spent a fair amount of time on on the phone. I wanted to talk about one in particular. This is somewhere along the

lines of what Lior has been talking about, that there may be some value to publicizing data. We heard a little bit about this in the health information panel. Robust databases can help provide meaningful research to be done in areas where we all may benefit. There may be progress in defeating disease if we all have good information, and yet, it does come at a cost. There are real trade-offs.

One issue that we haven't really talked a whole lot about is the risk that use of information in a way that individuals may find troubling will chill their conduct, will prevent them from reaching out using these Web 2.0 tools because they fear that their information will be gathered and potentially used against them. Whether this is a real fear that would come to pass or not, this is the fact that there may be chilling.

Would anybody like to speak to that issue? Jim?

MR. HARPER: Well, it kind of should, shouldn't it? The idea that you should be able to put out information and not have consequences is probably mistaken. Individuals should be aware. That's the most important thing. Understand what the consequences are. We don't know well enough, I think, with a lot of new technologies, a lot of new websites and protocols. But the important point is for people to be aware of

consequences and act accordingly.

MS. HARRINGTON-McBRIDE: Kathryn?

MS. MONTGOMERY: Well, I'd like to actually -- I know we already had a panel on health which, by the way, I thought was really, really interesting. But I would like to talk about one area in health that didn't get much discussion, and that's the way pharmaceutical companies are using the web and using digital technologies for direct-to-consumer advertising, some of which doesn't always look like advertising and often it's in the form of sort of unbranded sites that people might go to for information about symptoms and about illness.

I know all of us have probably had experiences where we either come back from the doctor with a diagnosis that we have to first learn how to spell and then want to know more about, and the doctor has given us information that's not totally clear or we have things we're worried about. I think particularly often with young people, sometimes these can be sensitive areas. They could be sexual issues, for example, about sexual health that they don't even feel comfortable talking to anybody about.

The online environment is a terrific one. Internet is a great resource for information. I use it all of the time, and I'm sure we all do. But in many

cases, you're not really aware of where you are and how that's being used and how that's being collected and, again, connected to other information about you. There's a whole infrastructure of companies engaged in this and people aren't aware of it.

I agree with Jim. I think if they knew, then they should be very careful about it. But this isn't as if you're sort of putting information out there. It's you're seeking information, and your very process of seeking for information, then, is part of what's being collected on you.

MS. HARRINGTON-McBRIDE: Anita?

MS. ALLEN: Well, I think it's often useful to go back to how we got the right to privacy in the first place. And remember that when Warren and Brandeis in the late 19th Century talked about privacy, they cited as the value behind it the notion of inviolate personality, the notion of mankind having a spiritual nature. I think that in recent times we've become reluctant to talk about those kinds of values in relation to data protection and privacy. But, yet, I think it does help explain why people feel that even when the data is out there and are public and accessible that they expect their fellow citizens to have too much politeness and manners and discretion to actually use the data.

I'm often surprised that my students will say, yes, just because I put it on Facebook doesn't mean that my employer has a right to use it. They assume that there's kind of a social norm, which doesn't exist actually, that people will just avert their eyes as to what they learn about you through readily available sources like Facebook.

So, I'm personally quite challenged by trying to figure out what do we do when, on the one hand, there is information out there; on the other hand, there are norms and shifting norms which might say you're not allowed to use the information just because it's there. You're not allowed to use it just because you could get access to it. There may be sort of rules of demeanor and deference and politeness that keep us from exploiting information in the employment setting and in other similar kinds of settings, that is there just because it's there.

MS. HARRINGTON-McBRIDE: This is Professor Helen Nissenbaum's theory of contextual integrity, the idea that there need to be some boundaries around which people will respect your decision to use information in one context, but not hope that it's used in another may be naive or aspirational, but, nonetheless, an interesting societal question.

I have one other question for the panel, and it's a toughy. We've talked a lot about the fact throughout the roundtable process, and even in this panel, about the fact that all kinds of information may be sensitive for some people. If that's the case, if the barriers and the distinctions between PII and non-PII are blending and data can be re-identified and there is this ability to take something that's seemingly innocuous to anyone, but maybe use it to access information that is not so innocuous about someone, does this get us into a world where all data is, in fact, sensitive? Is it the Midas touch idea that Parry has touched on? Is that where we now are?

Jim?

MR. HARPER: Well, I think most efforts to define sensitive data probably do explode; that is, there's almost no barrier because of contextuality and subjectivity. What it brings you to is an alternative way of addressing these problems, which is to focus on the harm that can be caused and then require whoever has data to be responsible in the use of it. So, go to something like the public disclosure of embarrassing private facts tort where you can get data, you can do anything you want with it provided you don't cross this line where the law defines the harm.

So, I think defining harms and saying, do all you want to do without causing these harms, is a more productive way of looking at things. It's more likely to allow innovations to occur. We can't now predict what future uses of data might be.

It's interesting to note, I think, that almost ten years ago, it was in May of 2000, the FTC came out with its report asking for legislation around notice, choice, access and security. In reading that over, you realize that this was before Google, it was before Facebook and Twitter, foursquare and everything else. If these rules had gone into place, knowing what we know then, would we have gotten those things? It's easy, in retrospect, to say, oh, of course Google would have figured it out. But Google looked like billionaire geniuses now and it's not a given they would have been able to do all of this stuff.

So, we are starting to learn what we don't know and I think a lot of FTC work has been good at exploring that stuff. I think it's important to not try to define, clamp down, though I think definitions of harms is a productive area to go to.

MS. HARRINGTON-McBRIDE: Okay. Lee?

MR. PEELER: So, I think Jim is making some good points. Just addressing the point that you were

racing about, are we saying that all information is sensitive? I think another way of phrasing that is to say, particularly in the commercial context, that we're saying all information should be treated fairly, and I think one of the things the FTC has done a wonderful job in over the last several years is creating some real expectations that information will be handled securely, and that if you don't accord information the security that its type suggests it should have, that you will be dealt with rather roughly by the FTC.

There's a great program right now ongoing with the revisions of the privacy notices to make the privacy notices more accessible. The FTC has led an effort that's been embraced by industry in online advertising to try to pull a disclosure outside of the traditional privacy notices to indicate the presence of online targeting, you know, an effort that the industry's embraced. So, I think if you're on the commercial side, there's already a lot being done.

The last thing, though, that I think is really important in talking about sensitive information is the educational efforts that the FTC has pursued. I was thinking about this last night because my youngest daughter called me and said that she was looking for a job this summer and a potential employer had said, e-mail

me your social security number. So, you know, I said, e-mail them your address, but let's mail them your social security number, and we had this big debate about why that was or was not appropriate. But, clearly, you know, that suggests a need for continuing education on these sensitive data issues.

MS. HARRINGTON-McBRIDE: We'll go to Lior. And then, Pam, if you could each take just about a minute, we're very close to overtime.

MR. STRAHILEVITZ: So, I'll try and be pithy and say, in response to your question, if everything is sensitive, then nothing is sensitive. Hierarchies in law are extremely important, not so much for automated processes. Automated processes don't get tired, but humans do. And if humans are forced to treat everything as equally sensitive, then the financial privacy, sexual privacy, private health information that we care about so much will get inadequate protection.

Just a quick point I'd make maybe by way of support for that statement is actually that we can learn a lot by looking to the law of trade secrecy which is essentially corporate privacy. And the judges there have figured this out. So, firms that stamp proprietary trade secret on everything don't get trade secret protection because the judges say you're overusing that label

sensitivity and by abusing it, you're not really sending a signal to your employees, to outsiders that this is to be taken really seriously. So, I think what the FTC has to do, even though it's a tall order, is to figure out what the hierarchy should look like so that we make sure that people do take those crown jewels of private information as seriously as they ought to be taken.

MS. HARRINGTON-McBRIDE: Pam, last word.

MS. DIXON: My comment follows on that very much. I was going to say it's really easy to decide, there's either all or nothing in this area. Everything is sensitive or none is sensitive. And I do think the solution is hierarchy and stratification.

I think a good example of this, even though there was a health care panel, is to think about health information in a little more detail. So, for example, within health information exchanges that are being done digitally, one of the large conversations that's taking place at the state level in every state in this country right now is what data, within health information, is sensitive data.

So, for example, there's a broad consensus that reproductive data, genetic data and domestic violence data, among some other types of medical data, are a little more sensitive in the hierarchy of medical data.

So, I think that it is possible to pull out categories of data within a hierarchical structure and at least begin there.

MS. HARRINGTON-McBRIDE: All right. Well, Michelle, we present you with a full plate of problems. So, it's up to you to solve them.

MS. ROSENTHAL: You did such a great job, I'm thinking of leaving this all to you.

MS. HARRINGTON-McBRIDE: It's these guys, not me.

MS. ROSENTHAL: You all did such a great job. So, over the course of roundtable series, panels have suggested a number of principles that might apply to the collection and use and sharing of data that would afford greater protection to consumers. I would like to touch on some of those principles and discuss whether and how they should apply in the sensitive data context.

So, I'm going to get to the fun one first. Some have suggested that some data is so sensitive that its collection should be prohibited altogether. So, Kathryn, is there any type of data or any type of user where the collection of that data should be completely prohibited?

MS. MONTGOMERY: Well, I don't know if I'd exactly say just the collection of the data -- in some

ways, I'm really talking more about behavioral profiling. I think it has to be looked at within the marketing context. A coalition of children's groups has called for no behavioral profiling for children under the age of 18 because of the special attributes of childhood and adolescence.

Now, saying that, I would not be talking about restricting access to information on the part of young people under the age of 18. I think we really have to look at ways to balance the autonomy and the freedom of young people to use digital technologies, which I think are wonderful, with some, I would say, restrictions on particularly what marketers do with their information.

Beyond that, I think, obviously, we need to ensure that young people understand what's happening on these various bases, particularly with social media marketing, where they are provided with new tools to set limits to their privacy and choose who their friends are and who has access to this and that, but they don't understand the entire apparatus of data collection and profiling that's taking place sort of behind the scenes there. So, I think we need to look at it. I'm not prepared necessarily to say this definitely, but I think it's an area that has to be looked at much more closely.

MS. ROSENTHAL: Okay. Lee, did you have

your --

MR. PEELER: So, again, we did work with Kathryn to come up with the existing COPPA format and regulations, and I think there's sort of two interesting learnings from that.

The first is that when the issue of industry self-regulation of online behavioral advertising came up, one of the issues was what do you do about behavioral profiling of kids, young kids, kids under 12? The response within the industry was that's a no-brainer. We have a COPPA framework, you would apply the COPPA framework to this area, even though the information doesn't meet the personally identifiable standards that currently exist in COPPA. So, the self-regulatory guidelines say, don't profile children under 12, under the COPPA standards, unless you have parental consent. It's not a prohibition because if the parents say it's okay to do this on this website after disclosure of what's happening, that should be fine.

But that's a good example, I think, of how, you know, again going back to first principles, there's a risk of harm to the kids and they are too young to deal with it. It makes it fairly easy on a going forward basis.

For kids, you know, 13 to 18, there's also some

interesting history, though. When we originally started the COPPA discussions, the proposal was to have COPPA extend to kids 17 and under, and that fell out of the debate. And it fell out of the debate largely because of concerns and uncertainty about just what Kathryn was talking about, what's the impact of that type of approach by the government on other pretty fundamental issues that involve what teenagers and tweens do and what their rights are and what their status in society is. And I don't think Kathryn is even suggesting that you would apply a COPPA model to young teens.

MS. MONTGOMERY: I'm not. Can I actually respond because I meant to say that?

MS. ROSENTHAL: Sure, go ahead.

MS. MONTGOMERY: It just didn't come out right.

MS. ROSENTHAL: Go ahead.

MS. MONTGOMERY: Because we dealt with this, Lee and I dealt with this. And I was really troubled by it. It was really challenging because the notion of getting parental permission, which, itself is a messy one. But I think the principle is what was important here and it has really helped to guide the development of the children's online marketplace.

But with teenagers, what I argued for was fair information practices directly for teenagers, which I

think is still important. Because what's happened -- because COPPA only applied to under 13, 13 to 17 is absolutely fair game with some of the most manipulative and unfair practices you've ever seen just exploding and really taking advantage of young people's need to develop identity, to explore identity, to explore friendships, to share and not really know. And even since then -- not know the consequences. Since then, there has been more science that has looked at brain development in teenagers. And we know that -- and this is actually reflected in public policy.

Anybody who is the parent of a teenager who is getting a driver's license knows that you don't get them as easily and as quickly as you did in my day when you turned 16 because the brain doesn't develop fully until into the early 20s and there is a tendency to be more impulsive, not necessarily to think about the consequences of what you do. There are also other things taking place in their social relationships. All of those things have been built into the marketing apparatus and there really are no fair marketing principles in place now.

MS. ROSENTHAL: Okay. So, you're saying there should be a baseline of principles that should --

MS. MONTGOMERY: I do, and I think we need to

really look at that and develop some policies.

MS. ROSENTHAL: Okay, thanks, Kathryn. So, Jim, there's been a concern expressed, this sort of ex ante concern, which is maybe in COPPA, COPPA is sort of -- I believe the magic words in COPPA are websites directed to children or with actual knowledge that information about children is being collected. But what about in other contexts? Do you always know that data is sensitive at the point of collection and how would this affect certain business models?

MR. HARPER: Well, you don't know. That was going to be -- my answer to your prior question was, no, there's no data so sensitive that you can ex ante say that it shouldn't be collected.

In a lot of business models existing today and a lot of those to come, which we don't know about yet, you don't know, as the operator of a website or a service, how people are going to use it, what they're going to say on it, what they're going to publish on it, what they're going to hand over to you, and whether it's truthful or not. I think that's the dimension of this that maybe people haven't thought about as much as they should.

Users are in a position, and I think they should be in a position to mask their identities that

they present to you, to mask the information that they present to you. They may say they are something that they're not and they're trying to achieve anonymity, pseudonymity, obscurity along one dimension, and that indicates to you that they're in a group that you have to deal with differently.

So, it's a real a mess to try to administer systems based on categories of sensitive information or categories of sensitive users, though I agree that you have to look out for sensitive users. I think COPPA is an example where the intent is certainly there to protect children. Whether it does or not, I think there is some talk about balance that should be done.

MS. ROSENTHAL: Mm-hmm, thank you. Lee?

MR. PEELER: From a regulatory, which I used to do, and self-regulatory, which I do now, standpoint, the point that you're making which is whatever standards you have have to be sort of predictable up-front is really important. Because a lot of the concerns we've been talking about today are things that may subjectively affect individuals differently.

So, you know, one of the things that's going on right now in response to the FTC's call is that the self-regulatory groups that develop the online behavioral principles have committed to continuing to look at the

sensitive information categories to see if we can't come up with sort of objectively defined criteria in the health and financial information areas to sort of further refine our analysis there. And that same work is being done by the network advertising initiative and has been ongoing for some time.

So, there really is an effort. I mean, the industry really understands that there are certain areas of sensitive information that require a higher level of protection and is working very hard to try to objectify that.

MS. ROSENTHAL: Okay. So, Pam, if it's difficult to prohibit collection, are there certain uses that should be prohibited? So, for example -- and I'll use the behavioral advertising context since we're talking about it a little bit. The way that the information is transferred from your browser to various servers, it just automatically is collected in many contexts. The URL is automatically given my IP address, it automatically goes to the server. So, the question is, in that kind of context, should use be prohibited?

So, if I decide to go to a sensitive website, to a website about -- I'm not going to use myself here. If someone decides to go to a website about sexually transmitted diseases, should that information be able to

be collected -- okay, it might be collected right because it's transmitted. But should it be able to be used to behavioral target that person?

MS. DIXON: Okay, this is a good topic. There's a lot of meat here. So, I'll try to be just as brief as I can. I really wanted to talk, in this context, about self-regulation and prohibition on uses. One of the issues -- I think, yes. I think that sometimes there is inadvertent collection and collection that is inescapable, for lack of a better way of putting it. In that case, yeah, you should have data retention guidelines that are applicable, and I think that is incredibly helpful, and also, data use guidelines that are very, very specific and concrete and say, hey, look, if you have it, you don't get to use it because there are direct harms associated with this. So, I think we can be very clear on that.

But I think something that also really needs to be mentioned here is the role of self-regulation in determining these guidelines. Currently, the self-regulatory process that has been in place for both the network advertising initiative and the IAB guidelines, both of them, there has not been enough tension in that process and industry has gotten together and made a self-determination what constitutes sensitive. The problem is

is that there has not been a mandatory addition of the consumer viewpoint. So, therefore, the definitions of what constitutes sensitive in both the NAI guidelines and the IAB guidelines are really incredibly weak and I think improperly so.

So, if we're going to have any kind of self-regulation in the sensitive area space, there's got to be some kind of joint rule-making or some kind of negotiated rule-making, something where there is some honest tension between what consumers want and what industry wants. Because if industry sets guidelines for what constitutes sensitive information, we're going to have weak guidelines just because we need more tension in the process.

MS. ROSENTHAL: Okay, thanks, Pam. Jim, go ahead.

MR. HARPER: So, there's a venue where this kind of tension plays out, I think, regularly, and that's the marketplace where participants, like Pam Dixon and many other advocates, point out that certain products and services are -- plenty of people on this panel, in fact, point out that certain products and services have negative implications if you share information with them. Look at this bad actor, look at this bad actor. Do you know what they're doing?

That's a really important process. And the important thing, I think, to me is that it's granular. It allows individuals to make the decisions. Of course, they encounter error. But they also make decisions for themselves about what risks they want to take, what services they want to enjoy at what cost to privacy or consumption of personal information, that kind of thing.

I think it's a far superior process, even though we're all great intellects, I'll include everybody in the room. We're all great intellects, but we don't have what it takes to figure out the optimal design of our privacy systems going forward. That's going to be in the marketplace.

MS. ROSENTHAL: Okay. I think that's a good point. So, there are consumers, obviously, that want to share information in certain ways. So, that sort of gets to another principle which is -- we've talked about restricting collection or use. But what about restricting sharing with third parties? So, an example I'll give is, you know, if you are on a social networking site and you decide that you want to play a game, let's say Scrabbulous. Does the provider of that game really need to know my religion and my political affiliation? Does all of that information need to be sent? And so, should there be certain restrictions that sort of prevent

sensitive data from changing hands?

I'll note that in the B2B context, many companies have these types of contractual restrictions. You know, they say, okay, we're sharing this data with you for this purpose, but you can't then go and use it. So, should this be a principle that we should apply to sensitive data? Kathryn?

MS. MONTGOMERY: Yes, I think it should be. I also wanted to respond to what Jim said, though. And that is that, you know, having been an advocate for a number of years and spent a lot of my energy and time doing research and working with the press and filing comments to expose bad actors and bad practices, it's a hell of a lot of work and it's not a very good system. It is a good system to be able to work as an advocate to try to influence policy. What we can do with policy is to create a level playing field so that consumers have a set of expectations when they're operating online and businesses have a set of rules. Now, that can be done through self-regulation, as well. But there has to be accountability built into it.

I think, again, the COPPA model of self-regulation and government oversight and government regulation has worked well. Whether the actual mechanisms are perfect, we can talk about. But the idea

of a framework of government regulation that then operates with some rules of the game that have resulted from some consumer input, so that we can have clear expectations.

So, the other thing is, you know, who has seen a privacy policy lately and been able to decipher it? You know, you can't -- and the other thing is it's not a question of whether you're going to be able to negotiate with that website or with that service. It's take it or leave it, essentially. And a lot of these are services that we all need and they aren't exactly alternatives. I don't think the marketplace has worked.

MR. HARPER: Just in brief --

MS. ROSENTHAL: Parry. I want to give Parry a chance to answer. She's had her --

MR. HARPER: A brief response if I could.

MS. ROSENTHAL: Yes.

MR. HARPER: I don't want to diminish what Kathryn says, but that's exactly what an advocate would say about the system. It's never satisfactory.

MS. MONTGOMERY: And that's exactly what you would say.

MR. HARPER: Neither is it satisfactory to people on the other side. I'm an advocate and I'm dissatisfied with the Obama administration's privacy

practices, for example.

MS. ROSENTHAL: Thank you, Jim. Parry?

MS. AFTAB: I think as we start looking at this -- I'll make one brief comment on the advocacy role. I think that a good appearance on the "Today" show will change a lot of website practices pretty fast and sometimes better than our sitting in a room and negotiating for months with different people who are not doing what they're supposed to do.

But that said, I think that if we start looking at this third-party sharing, I think if it's an unexpected third-party sharing that we should be regulating that. And if it's the kind of thing that isn't open, it's not on your Facebook profile and open to the world because you're not using the privacy settings and anybody could have seen it, I think that that can be done. And when you look at the B2B environment, which you can turn around and say, I'll share information with you, but you can't share it with others, it's only for our purposes or this limited purpose that we do, that comes under expectations, everybody understands what it is.

But when it's something that's already available to everyone, it's hard to restrict it. So, I think, as we start trying to see if that could work,

we're going to have to be very granular. Is it information that's already covered and protected by privacy settings so that the person's locked it up? Is it the kind of thing that the person has restricted? Have they provided, in effect, expected consensual use by anybody who happens to see it? I think as we do that, we can come up with a solution that restricts the third-party use, as long as it's expected and defined and in the kind of thing that people would assume that it's not otherwise available just because I have the user access, a log in and password because that's how they're going to get on to my social game. I'm not going to be able to get in and see other things that they're posting that they're keeping private.

MS. ROSENTHAL: Right, okay. Anita?

MS. ALLEN: Well, I don't think that the average Jane or Joe consumer knows how their Toyota works, and they certainly don't know how the Internet and the web work. I think that we really need to have a very strong kind of consumer protection mentality when thinking about these issues of collection, use and sharing with third parties. And while, in some idealistic political world, maybe we would have a complete free market and let people just make their own contracts and their own bargains and do their own thing,

but I think there's so much complexity, so much technical complexity, so much hiding of information and unavailability of information and so much lack of freedom to truly bargain with website operators, for example, that we really need to have the government here playing a very strong role.

I think the FTC needs to play a very, very strong role in regulating the ways in which information is made available and not available. I don't think that we should be too reluctant to use coercive and even paternalistic measures at this stage of life. The Internet, the web, is too new for us to assume that people are capable of taking care of themselves when it comes to their online transactions. I personally welcome a bit of someone else kind of helping me through my financial and market transactions on the web, and I think that the FTC has a very important role here.

MS. ROSENTHAL: Thanks, Anita. What about -- there's the principle of sort of minimizing data collection? So, I'm going to borrow an example from Jules Cohen from Microsoft earlier today where he sort of talked about, you know, you go to a bar. Does the bar really -- I show them my license and all they really need to see is my date of birth. They don't need to see my address. They don't need to see my license plate number.

So, I should be able to give only the amount of information that I need to give and that additional sensitive information or potentially sensitive information shouldn't be collected.

So, Lior, what kinds of harms would this type principle protect? Is this a good principle and would this protect against certain harms that we discussed in the first portion of the panel?

MR. STRAHILEVITZ: Well, in a lot of the web-based applications, the consumer has a variety of self-help options which turn out to be fairly effective. So, a colleague of mine on the faculty was in his office about two weeks ago and he's searching for a condominium in Chicago. I had turned him to a really nice real estate website that helps people find condominiums in Chicago, or houses, too, I suppose. In any event, he's searching for condos and gets a call on his phone. Oh, I see you're looking for two bedrooms in the blank blank neighborhood in Chicago. And he tells me this story and I said, you mean you gave them your real name and your real phone number?

So, part of what I think individuals do in these circumstances -- and this is a falsifiable hypothesis -- is they get around regulations they don't like by providing incorrect information. And I think

firms that are doing work in this area, tolerate very high levels of what we'll call consumer self-help on pro-privacy perspectives.

The other thing that happens, I think, through this sort of interaction is a consumer was very ticked off by what he viewed as an intrusive search into his own internet usage patterns and decided that next time he looks for a condo he'll use another website, which does suggest that these market forces can work, but only if the fact that there was a person who was scrutinizing what my colleague was searching for by way of real estate, only if that becomes transparent. So, it's the stupid firm that says, I see that you're looking for condos in this and this neighborhood. And the danger is when that monitoring can be both surreptitious and potentially threatening or harmful to the consumer in some ways.

But having said that, I think the popularity of self-help through allowing consumers to provide inaccurate information or only partially revealing information about themselves does suggest that there's a fix here, and one interesting legal question is, how should we regard my decision to enter Donald Duck as my user name. Is that a breach of contract? It might well be under the terms of service. Or is it something that I

would be empowered to do as a way of opting in to a privacy arrangement that's more protective than the ones that the firm on the other end of the transaction seems to be offering me? If they tolerate me as Donald Duck and nobody ever calls me on it and I'm allowed to continue using the service, should we regard as me having amended the contract and them having agreed to it by continuing to provide me a service? That actually strikes me as a very interesting legal question on which there's good thinking to be done.

MS. ROSENTHAL: Thank you, Lior.

I'm mindful of the time. We have about 15 minutes and I would not want to take up anybody's break time. So, I'm going to try to quickly get to some of these very important principles. What about limiting data retention, Parry, what kind of harms would that prevent?

MS. AFTAB: Well, I think limiting data retention is a little bit what you were talking about at the bar.

MS. ROSENTHAL: Right.

MS. AFTAB: When we started looking at pornography and whether or not you could require someone to prove that they were over the age of 18 to be able to see certain pornographic images. It was thrown out

because we said you might have to flash your driver's license to show that you're 18 so you can buy a magazine, but if you're flashing it online, somebody is collecting it. Then once it's collected, it's being used. And I think they really come together.

So, I think that as we're looking at data retention, it could be it expires after a certain time, after the right use. It could be that it's tagged and watermarked in effect so it can only be used for certain purposes as it moves. And it could be that it comes through authentication and smart card type of technology that it contains the information, all they're doing is authenticating somebody's 18, somebody is 13 and capable of COPPA communication, somebody can have this communication without the sites actually having the real information. They're just having the authenticated fact that somebody's met a threshold. So, I think it works that way.

MS. ROSENTHAL: Okay. And should it only apply to sensitive data or should that be the type of principle that applies across the board?

MS. AFTAB: You know, I really think that if we start applying it across the board on things that could be sensitive under certain circumstances, and if we can get enough people to adopt it, I think it works. I think

it’s finding trustworthy providers, so the companies providing those smart cards or authenticated services, you know that they’re not going to have the data bleeds and they’re not going to have -- you know, they’re going to have adequate security and the right rules in place to govern it. But I think if you do that, it might be an answer to a whole bunch of the harms that we’ve identified.

MS. ROSENTHAL: Great. Okay, thanks. So, we talked a lot, I think, in this panel about subjectivity and what’s sensitive to me may not be sensitive to Katie or vice versa. What about the principle of access? Would access prevent sort of that concern because it would allow consumers to -- and, of course, we have to talk about what access would look like. And I know there are a lot of feasibility issues and operational issues and things that would need to be discussed. But if I can access the type of data that a company has about me, and either edit it or suppress it if it’s incorrect, would that prevent against or at least mitigate certain harms, especially some of the harms that are less concrete? So, you know, the dignitary harm or reputational harm. Pam?

MS. DIXON: Yeah, I think the access model, especially if you look at the Fair Credit Reporting Act model and how that works with credit bureau reports. I

think it's a very, very good model to look at and I think it's a challenging model to scale to a broad Internet kind of site issue, but I don't think it's impossible. I think certain principles could be extracted and applied. I think it's a very helpful way of thinking about it. I think that something else along these lines that I'm thinking about. Just to follow in the last conversation, identity management I think is going to be a real issue when it comes to sensitive data in certain categories. Financial and medical come to mind because you have to authenticate the person, then you have this authenticated information laying around.

I think that we should not minimize how incredibly sensitive that information is, in and of itself, as a category. From this morning's panel on identity management, I think we need to look at identity management as a coming, very significant issue that's going to need a lot of thought and attention and may be itself considered its own category of sensitive information.

MS. ROSENTHAL: Thanks, Pam. So, Lee, is there a cost to access -- you know, what end kind of cost is associated with access and can we really expect small companies to engage in this type of practice?

MR. PEELER: I mean, that's exactly right. I

mean, unless you're set up to provide access there could be very significant cost in providing access. And also, you could increase the privacy harms. Much of the information that companies retain now is in machine-readable form and translating it in a format that a consumer could actually get it and understand it would entail making it more vulnerable to start with.

And then anybody that's been through the credit bureau report disclosure process knows that just verifying that you are who you say you are, in light of the very significant threats of identity theft, requires you to disclose a significant amount of information, in and of itself. And if you don't get that balance right, you could end up disclosing sensitive personal information to someone who's not entitled to it. So, I think you need to be sort of wary of these broad one-size approaches.

MS. ROSENTHAL: Thank you. Thanks, Lee. So, I'm going to move on. This next question is for Anita. The principle -- I think the most common is sort of the principle of transparency. It's one that we embraced in the behavioral advertising principles in the report and sort of the idea of notice and consumer control and sort of making sure that consumers really understand what's happening. But, Pam, you know, the question is, can

notice truly convey the nuances of the various business models and some of the long-term consequences. So, maybe there's not a harm that's going to occur tomorrow, but maybe it will happen over time and specifically some of the harms that may accrue as data is aggregated.

MS. ALLEN: Pam or Anita?

MS. ROSENTHAL: Did I say Pam? I meant Anita and I said Pam. Apologies. You're sitting right next to each other.

MS. ALLEN: Well, transparency is great for consumers if they can then use the knowledge they acquire through genuine transparency to affect change in their life and protect their interest. I mean, one problem is that transparency without some sort of entitlement or privilege or right to do something about what one discovers is not very helpful, much in the same way that access without the capacity to actually change is not very useful.

I can recall once getting my credit report and discovering that my name was not Anita, but Danita. Every bit of financial data was absolutely accurate, but my name was wrong. Even after I sent my passport and my driver's license, it took me a year to get my name changed from Danita to Anita. So, access without the power to correct is not very good. Transparency without

the power to then affect the institutions and practices and information to make things right is not going to be any good either.

MS. ROSENTHAL: Lior, based on all of these principles that we're discussing, do we really need notice? Do we need to give all of this information to consumers? If we had sort of a baseline, sort of a level of protection in various principles that we think are actually protecting consumers, do we need to provide notice about every specific piece of data that's collected and used?

MR. STRAHILEVITZ: Well, not if you phrase it that way.

MS. ROSENTHAL: So, we just need really good protection?

MR. STRAHILEVITZ: Well, here's what I think we need to do. So, with any consumer good, you're going to see bundling of various services into categories. So, people don't buy cars a la carte. They purchase the premium package or the premium plus package or the fat cat package or what have you.

I think this bundling, in terms of privacy law, can be very helpful to consumers. So, if you think about let's say what Microsoft does with respect to its software, you can opt for a high security, medium

security, low security. That's a useful way to think about meaningful choice to consumers.

What I think the law needs to do, though, is make sure that high security really is meaningfully more protective than medium security and that low security is meaningfully less protective than medium security. I think sometimes, because consumers latch on to labels and short descriptions, much more than they are likely to latch on to details or have time to read the details, we can actually make a tremendous amount of progress with these short descriptions and then the law's role is simply to make sure that the terms actually match the abbreviated descriptors for the substance of what the consumers are buying when they're agreeing to a particular service.

MS. ROSENTHAL: Thanks, thanks. What about in the consent? Pam, you know, the argument has been made that if you were to require something like an opt-in for sensitive data that, A, it would ruin certain business models. It would actually prevent them from doing business the way that they do it. But also that consumers are going to opt in. That if you give them the right incentive that they will opt in without truly understanding what they're opting into.

MS. DIXON: Yeah. I think consent is a really

challenging issue. Consent really isn't a 100 percent solution for sensitive data because it can be manipulated. It has to be done very, very carefully. So, that would be my answer there. It can be done, but it has to be done very carefully and cautiously. In terms of notice, I do think that notice is very important. We need a public dialogue about this data. And too often, consumers do not have enough information for the dialogue.

MS. ROSENTHAL: Thanks, Pam. Jim?

MR. HARPER: I would just say on both these ideas, transparency and consent, they're both great ideals. I think transparency is essential. It's not essential for each individual user of a service to take advantage of the transparency immediately. We have an Internet-y problem here and it needs to be solved in an Internet-y way.

MS. ROSENTHAL: Did the court reporter get that?

MR. HARPER: Internet-y. It's a new adjective, I didn't come up with it.

But a broad, diverse, moving, changing community will make decisions about what's appropriate to do, about what services are appropriate to use. It's a distributed process and consumers are very well

positioned, thanks to the Internet, which is a communications medium to learn about this stuff. Many don't. We're never going to be satisfied that everybody knows enough, especially those of us in the room. We're never going to be satisfied that people are intellectual enough about their privacy decisions. But collectively overall they'll do a better job of figuring stuff out with the help of their peers, their colleagues. I'm proud of the fact that my dad told me to use Amazon the first time. That was because he'd gotten advice from others that this was pretty cool. So, I went ahead and used it. That's why I used Amazon, not because I read their privacy policy or investigated Amazon. The collective mind had investigated Amazon and gave it their stamp of approval.

MS. ROSENTHAL: Thanks, Jim. So, Parry, what about security? Commissioner Harbour mentioned this morning, sort of using SSL for email. I think that sort of raises a good point, which is we talk about -- I talked with Jim about the ex ante concern, which is you don't always know that it's sensitive before you collect it. But I guess we could probably all agree that your email contains some sensitive information. Certainly, those that don't have Lee as our father might include information that might be deemed sensitive, perhaps

Social Security numbers or information about your medical information and what have you.

So, would this address sensitive data -- should we expect -- you know, should e-mail providers use this type of encryption just because they know that the odds are there is sensitive data included in email?

MS. AFTAB: No.

MS. ROSENTHAL: No?

MS. AFTAB: I think that it's less about what you're sending by e-mail and more about what happens to it once the data arrives.

MS. ROSENTHAL: Okay.

MS. AFTAB: So, you see a lot of issues where people have access to it and people have no idea who they are. There's no background checks. So, people have access to the data. They have no control over the computers. Maybe somebody is doing it remote. You've got moderation staff who are working remote or in other countries and nobody knows who they are and where the computers are and who else they may be working for and confusing it with. So, I think it's a lot less about the channel of e-mail and what's being sent and a heck of a lot more about training practices, processes, policies, good old-fashioned data hygiene when it arrives.

MS. ROSENTHAL: Thanks, Parry. So, we have

about two minutes left. So, I'm going to get to the final question. During the first half of the panel, we discussed the considerable challenges associated with defining sensitive data and the concern, of course, that if we label everything sensitive that nothing is truly sensitive. So, recognizing that, we also discussed a number of principles that should be applied to the treatment of sensitive data. And some of you suggested that a number of these principles might apply to all data despite whether it's considered sensitive.

So, let's get to Lee's point which is something that he mentioned earlier which is, is there some baseline level of protection for all data that would obviate the need for special treatment? Should we just be applying these principles across the board and feel that the then sensitive data will be okay, that we shouldn't be concerned about sensitive data because there are certain principles that would apply to all data.

Pam? Pam and then Kathryn.

MS. DIXON: Yeah, I don't think we get to go there in the sectoral society that we have running here. I think that certainly one can look at Europe and say, you know, the omnibus style of protection is a model that could be very seriously considered. But the reality in this country is I don't know how we could institute that

at this point in an easy fashion. Maybe it will happen someday, but it isn't here today. So, let me just speak about today. I think that today in our sectoral system, I do think that we need some kind of sensitive data protection. I think we're going to have to work very hard to create hierarchies that make sense and I think it's going to be very difficult to find one single standard and say, okay, absolutely, everyone on the Internet and the health care sector and the financial sector, you all meet the same standard for all data. I just don't think it will happen.

MS. ROSENTHAL: Thanks. Kathryn?

MS. MONTGOMERY: I think we've got a very challenging situation as I look here at the principles of data minimization and rules about data retention and access and transparency. I think we have the opposite system that's emerged in the digital marketing infrastructure. It is all about data maximization. it is not at all transparent. There are many, many, many forces at work that are going in that direction, and at the same time, I think we should think about the goal of a broad set of rules that will mitigate some of these very strong forces.

But I don't think it's either/or. I think we should seek that, push for that. But I think we also

should be developing, and it's probably going to be a little bit more manageable, even though it's going to be complex and we haven't resolved it all, some ways of addressing these sensitive issues and sensitive information. I think that can be done. We're not going to solve it all today, but I would urge the Commission to pursue that.

MS. ROSENTHAL: Thanks, Kathryn. Jim, you get the last word.

MR. HARPER: Well, thank you very much. I'll be brief. If there's a baseline --

MS. ROSENTHAL: Oh, I'm sorry, I didn't see Anita.

MR. HARPER: Second to last word.

MS. ROSENTHAL: Yeah, second to last word.

MR. HARPER: Because this is a real zinger.

MS. ROSENTHAL: I know, I'm sorry. You want Anita to go first?

MR. HARPER: No, unless Anita had -- if there's a baseline rule that should apply to all collectors and holders of data, it is that they should be subject to the rule of law. And I speak especially of the United States Government, which essentially steals data and it has not seen any sanction as of yet. Zinger. I told you.

MS. ROSENTHAL: Wow, that's a zinger. So, Anita, you got to top that.

MS. ALLEN: I am so glad we're not stopping there.

(Laughter.)

MS. ALLEN: Sensitive data is not a plutonic essence. But I think we need to keep using the concept. It's a rule of thumb. It's a heuristic device for helping us to remember that there are important social values that we incorporate in our data practices.

MS. ROSENTHAL: Thank you, Anita. We have to end.

MS. AFTAB: Just one comment.

MS. ROSENTHAL: Yes.

MS. AFTAB: Yes. I think that, two things, A, privacy and respecting users is good for business. We need to remember that. But the most important thing is, the two of you have done a remarkable job.

MS. ROSENTHAL: I'm glad I let you go, Parry.

MS. AFTAB: But throughout this entire process, how you worked with all of us, how you pulled us together, it's like herding cats. You made sense of this. You basically kept to time. But I think that you two are amazing people who really brought this whole thing forward today. So, thank you.

MS. ROSENTHAL: Thank you.

MS. HARRINGTON-McBRIDE: Just for the General Counsel folks who may be in the office, I just want you to know that this was not a paid endorsement.

MS. ROSENTHAL: We did not pay her.

MS. HARRINGTON-McBRIDE: We don't want any sort of concerns arising.

MS. ROSENTHAL: Thank you. You all have been wonderful and we really appreciate all of your work. Thank you.

(Applause.)

(Panel 3 was concluded.)

PANEL 4: LESSONS LEARNED AND LOOKING FORWARD

MS. MITHAL: Okay. Well, thanks, everybody. We are now in the home stretch, the final panel and the final roundtable that the FTC has been hosting over the last several months. Those of you who have stuck it out will not be disappointed. We have a very distinguished group of panelists with us. And let me just introduce them down the line.

We have Paula Bruening from the Center for Information Policy Leadership. We have Fred Cate from Indiana University School of Law. We have David Hoffman from Intel; Chris Hoofnagle from Berkeley; Richard Purcell with the Corporate Privacy Group. We have Jennifer Stoddart, the Canadian Privacy Commissioner, and we also have John Verdi. John is filling in for Marc Rotenberg who was called to testify before Congress. So, John is a last-minute replacement and I'm sure he'll do a great job.

So, before we get started with the substance of the panel, I thought I would just start with some opening notes. First, the title of this panel is lessons learned and the way forward. So, the way we'll do this is we'll be picking out nuggets of things that we've learned at the prior roundtables and we'll be exploring them and talk not about challenges, but mostly about the way forward and ways we can address the challenges that have

been raised. So, I urge the panelists to kind of look forward and talk about the future a little bit.

Second, we have a lot to cover in this hour and a half. So, I'd ask the panelists to keep their remarks brief and to the point. And, finally, since we have a lot to cover, I just want to be clear that the issue of government collection and use of data is a really broad one and that's something that we won't be covering today. So, if you could keep your comments restricted to commercial collection and use of data, I think we'll be able to get through the material that we have.

So, with that, let me just start with the first question. We've heard a lot today, and in prior days, about the distinction between personally identifiable information and non-PII, how it's been increasingly blurred. And I want to throw the first question out to Richard Purcell and ask him, is this PII distinction still viable? Is this something that we should continue to use in our vocabulary as we talk about data collection practices?

MR. PURCELL: Thank you. Personal data has become ubiquitous in all of our society. I was speaking with Dana Boyd, a Microsoft researcher, who was referred to earlier as well. She had a really interesting comment. Her observation is that decades ago, not that

many decades ago, what was easy was being private and what was difficult was being public. In today's world, that's reversed. It's overly easy now to be public and very difficult to be private.

One of the things we've discovered is that all data has personal implications. If it can be linked to a person, not only can it be, it will be with some inevitability. I believe that any bit of data about an individual deserves the kinds of protections that we currently reserve for personally identifiable data largely because, inexorably, maybe not today, I'm sure somebody could make a big argument that would say, no, no, no, we can actually have non-PII. It's going away. That distinction will no longer be relevant in our future.

Since that is a case that I think we can all commonly agree on, that at least in the near term, sometime in the short-term future, all personal data will ultimately become identifiable or attached to an individual, that all data about people needs to have protections, needs to have consideration, needs to be protected in some way or other.

It would be -- it's a little bit like confidential data at a business. If it's about the business, there is a chance that it needs some kind of

discretion, exercised around it, period, end of story. If it's about intellectual property, if it's about processes, any of that, what we call maybe trade secrets, then it needs to have protection and discretion has to be applied. If it's about a person, at the very least, we have to be discreet about how we use it. So, for the future, I think yeah, there is no such thing as non-PII. It just should not be treated differentially. It's all roped together.

MS. MITHAL: Commissioner Stoddart?

COMMISSIONER STODDART: Thanks. Yes, amazingly enough, in Canada, we never made that distinction. We just talked about personal information. Then some of our American colleagues started talking about PI and PII and we had to say, well, what is that? Kind of try and munch that one over.

But what we do in Canada -- first of all, I think the work of people like Latanya Sweeney was carefully studied and the lessons have made a big impact on Canada, even about ten years ago. So, we avoided going to a very tight distinction between the two. And then generally in Canada, we use concepts like proportionality, context, how the law is applied, what the outcomes are to be, to modify whatever the principle is. So, I'd just like to tell you what our own federal

court said recently, almost paraphrasing Richard, in a case where we proposed this test and it was adopted.

"Information will be about an identifiable individual where there is a serious possibility that an individual could be identified through the use of that information alone or in combination with other available information." The information that was being contested in that case, it was about drug trials and government-held information on drug trials. The particular piece of information that was withheld was the province. The province is not personally identifiable information, in itself, probably, but combined with everything else would have let the media learn about who had died in a drug trial. And so, in that case, it was adopted. So, that's how we approached it. Everything is potentially personally identifiable information.

MS. MITHAL: Well, let me ask a follow-up question and then I'll get to David and Fred. So, suppose a company says to consumers, we collect your information and share it with third parties on an anonymous or aggregate basis. Given what you all have just said, does that create a false sense of security for consumers?

So, I'll call on David and Fred, and if anybody wants to answer that question or address something that's

been said before.

MR. HOFFMAN: I think the answer to that is it depends. I think there are ways to anonymise data or de-identify data, but depending on how that data is then going to be used and whether it's combined with other data, could potentially have it relate to an identifiable individual in the future. I think the debate over is it personal data or non-personal data, is it PII or is it non-PII, is something that we have spent a tremendous amount of time, as a privacy community, debating for maybe the past five years especially, and I think it's largely been an unproductive debate.

I think most of the place where the debate has happened has been in Europe on the definition of what's personal data in Europe, particularly with respect to IP addresses. IP addresses I find to be interesting, particularly for the company that I work for, because what an IP address really is is it is an identifier, and most often, a unique identifier at least for a period of time that's stored in hardware or software. Well, there's actually a great number of instances of similar identifiers.

So, I think the question -- you know, under the implementing legislation of the 9546 directive, what's interesting in Europe is the definition of what's

personal data. What's something that can relate to an identifiable individual and things that could likely reasonably relate to an identifiable individual, when combined with other data in the future. I think it's fairly easy to see that many of these identifiers that could occur in hardware and software could potentially fit into that category.

So, the question is then, so what? I think -- and this is what I think is really important to be learned from that debate, which is that the reason why so many organizations and entities needed to come forward and to try to fight that was because the restrictions that would be imposed upon them then if a certain category fell under the definition of personal data, under some of the nation states implementing legislation of that directive was deemed to be very burdensome. I'm not saying whether I think it was or not. I'm saying that it clearly was by others.

So, for example, people make the argument that under the UK law, the existing UK law, that if something falls under the definition of personal data, then an individual has a right to get absolute access to all of the processing of that. If you think about that in the terms of a unique identifier and hardware or software, it may actually be extremely difficult, if not impossible,

to actually even be able to provide that to an individual. And even whether -- if it is possible. you'd have to ask the question, well, does it really make sense for them to know all of the logs everywhere, where every IP address is that could relate to them and how are we going to authenticate that individual to come back to see if it really does apply.

So, once again, I think what this really comes back to is these definitions make a lot of sense if we have flexible, normative standards that are applied on top of them that really make sense for the degree of protection that's necessary for that type of data, which I think is something that Richard and Jennifer were both talking about and I wholeheartedly agree with.

MS. MITHAL: Fred, I'm going to give you the last word on this and then we'll move on to the next topic.

MR. CATE: Thank you very much. I would certainly echo the point on proportionality and just say I think we might add to that the notion of contextuality because you would have to say PII for what reason. So, for example, our Freedom of Information Act exempts certain data that might be thought to threaten privacy. Well, if we said all data concerned was personally identifiable, we might exclude all data from that, or

access. The example's already been given. If we apply access to all data that we think could be used to identify you, we would then make access meaningless.

So, instead, I think this notion of proportionality applied in context and I think maybe the best example there -- and it's one in an area already been touched on today -- is in the area of health information. So, for example, for years companies that do health research dealt with what we would call anonymised data, meaning they knew exactly who they were dealing with, but they were required by the FDA to screen that identity behind a number and that number could not be applied to de-identify the data under threat of federal penalty, except in certain circumstances.

So, most of us would refer to that as de-identified data. Yet, of course, technically Latanya Sweeney would tell us that is fully identifiable data. The point is irrelevant. In other words, it's a question that I suspect has no meaning any longer, rather we come back to this question of what is the broader context and what is the proportional response to whatever we come up with out of that.

MS. MITHAL: Okay, thank you, Fred. I'd now like to move on to transparency. We've talked a lot about notice and choice at these workshops. Actually,

they've probably been fairly vilified, the idea of long privacy notices that consumers can't understand, that they don't read, and if they read them, they can't understand them. But I would like to direct this question to Fred. Is there a continued role for notice, and if so, how can we make notice meaningful?

MR. CATE: This is so hard. Let's face it, I mean, notice and choice have not only being vilified, somehow they manage to continue to survive. I was going back looking at the record. Every chair of the Federal Trade Commission since Chairman Muris has expressed dissatisfaction with notice. Yet they seem to hang on. I mean, like what do you have to do to kill something around here?

(Laughter.)

MR. CATE: They keep coming back. At the beginning of the last of these three roundtables, David Vladeck began by saying, there's still an important role for notice and choice. And I find myself scratching my head saying, what is that role? So, I guess there is some role left for notice. But what is that role is, I think, a very hard question.

So, I would say one of the things that many advocates point to notice for is it tells the rest of us, just the few of us in this room, nobody else outside

could care less about what we're talking about. But those of us who do, it tells us what companies and government agencies are up to. So, in that sense, if we just mean transparency or regulatory filing, like you have to tell the FTC what's your privacy policy, yes, I think that is a continuing valid role for notice.

Another area where notice, I think, has clear continuing validity is where there is a meaningful choice for an individual data subject to make. So, if you're actually going to ask me, do you want your data used and point this way or that way, you got to tell me. You got to give me the notice or else that is a completely pointless illusion of a choice. So, in that one instance, individual notice might make sense.

And then a third rule for notice, although I would never use the word notice for this ever, but just because somebody else might and I don't want to feel like I've left something critical out, I think there's an educational role for notice. So, again, I would not call this notice. But, again, let's face it, most people are not interested about being educated about how their computer collects data about them or how business collects data about them in the environment. But for those people who are or in those settings where we really think it's important that there be education, notice of

some form probably plays some role in that education. Those would be my three suggestions where notice would remain valid.

MS. MITHAL: Okay. Reactions, John and then Chris?

MR. VERDI: Sure, yes. I would agree with the widespread derision regarding notice and the notice and choice model. I think that what we really have at this stage is an understanding that control and access and meaningful and effective privacy safeguards are what consumers expect. They're what good businesses provide and they are something that needs to be required. And I'll just tell a brief story about one of the more recent failures of notice, you know, and notice and choice.

There's a company out there called Echometrics which publishes a piece of software that parents can purchase and download and limit the access of their children when their children surf the web. It's safe surfing software, right? And this company also has a sideline in selling all of the data about the children that it's "protecting" to marketers so it can profile them without telling the parents.

But here's the issue. We ran into this issue, and the issue was brought to the attention of the Department of Defense. And it was brought to the

attention of Department of Defense because the DoD had agreed to sell the software to military families at a discount. So, you could get your Spyware cheaper. And what we found out was, once the DoD became aware of this situation, they began making inquiries with the company and they said to the company, why are you doing this? This is inconsistent with our principles, this is inconsistent with fair information practices, et cetera, et cetera, et cetera. And the company said, well, there's this check box and you can check this check box. And it's buried a little, but it's in there somewhere. And you can opt out of all of this data collection.

And the DoD responded by saying, we only permit personal information to be collected in order to improve the quality of the service. You've purchased product, we're going to collect personal information to improve the quality of service. Fine, fair enough, everybody can get on board for that. Just by giving someone notice and the choice not to check the box, that isn't good enough.

So, I think that that's sort of a common sense principle that we see in real life. You know, you drop your car off at the gas station for service and they drive it around if they need to to figure out where the rattle is and they replace some parts and they take some things apart and, hopefully, they put it back together

and all that fun stuff. But if they decide they're going to take it to Florida and then they're going to drive it back, you know, I mean they explicitly didn't prohibit that when you entered into that agreement, but there's sort of a common sense understanding. They're going to do what needs to be done to provide the service. And I think data collectors need to be doing that as well. Notice and choice doesn't allow you to collect data and use data and transmit data and share data and disclose data in ways that are wholly unrelated to the service and not beneficial to the consumer.

MS. MITHAL: Chris?

MR. HOOFNAGLE: I would agree with everything Fred said and go on to say that we need to -- if we are going to pursue notice as a solution, I think we need to change the incentive structure in the notice format. I've just noted that every time that I go online to pay my telephone bill, it interrupts the payment process to ask me if I want to go paperless. Every single time. And that is so important to them that they're willing to interrupt the payment process. I'm about to give them money and they say, oh, before you give us money, we'd like you to go paperless.

The other kind of example that I would bring up comes from Chase Bank. They wrote a notice concerning

overdraft fees, if you want to opt in to overdraft fees. And the notice that they wrote reads, “if you do not contact us, your everyday debit card transactions that overdraw your account will not be authorized after August 15th, 2010, even in an emergency.” This is written in red and underlined. We don’t see privacy notices that say anything that clearly or that urgently. And I would argue that it’s a problem of the underlying incentive structure.

MS. MITHAL: I see, Paula, you raised your tent. And I’d like to actually direct a specific question to you. Fred raised earlier the idea that maybe notice is useful when there’s an opportunity for a consumer to make a meaningful choice. So, just broadening that a little bit, are there things that we can take off the table in notice so that a notice might be more readable to the consumer?

MS. BRUENING: Well, I think that one way to think about notice is that there may be two kinds of notices that we might be able to offer. And I’d just like to preface that by saying I agree with Fred’s analysis, that notice remains important for all of the reasons that he stated. But I think there are two ways you can think about this.

Indeed, notice is at its most useful when there

is something meaningful going on where you can truly consent where there's really a choice that the consumer has, but that doesn't happen all of the time. So, it would seem that to maintain the transparency, you'd want to have some kind of an available notice, where we can all, wherever we sit, whether it's in government or it's policymakers in this room or it's the average person sitting behind their computer screen, they can find out what's going on within a company in terms of their data collection practices and their privacy protections.

I would say that there's also an opportunity for notice where there's actually going to be a real choice that a consumer can make. That's what I would refer to as something we call just-in-time notice. At that point, you can offer to the consumer the information they really need in order to make a meaningful, well-considered choice. Now, what those particular pieces of information are that they need, that probably remains to be worked out. But I think there's work to be done to figure out what does the consumer want to know, what really underscores a good decision and then figure out ways that you can make that available in realtime when the data collection is actually going on and when there's a real decision to be made.

MS. MITHAL: If I could just follow up on that.

We've heard about this concept of just-in-time notice before. But I want to kind of bring it back to Chris' point, which is every time he makes a payment, he's inundated with that request of whether he wants to go paperless. So, is there a concern about consumers being provided too many notices, being inundated with notices at the just-in-time point? I can ask -- Paula, you can answer that or I can -- or David or Jennifer?

MS. BRUENING: Well, just as a quick response, we probably don't have as much choice as we like to think that we do. So, if you really put the notices in front of people when they actually have the choices, it may not be as many notices as we might think. The important thing, though, is that behind that just-in-time notice is something more robust, that's more comprehensive so you can really get the entire picture if you want it. I would argue that probably most people aren't that interested in it, but it does provide the transparency. And that broader notice is also available in cases where there really isn't choice, but you just want to know more about what's going on as does the FTC and other people who are in the advocacy community.

MS. MITHAL: Okay. David?

MR. HOFFMAN: I was just going to try to answer the question and state specifically some things that I

don’t think serve a lot of purpose in notices anymore. I think there’s been some fantastic work that’s been recently done on a use-based model around privacy, and a lot of that work has been to delineate certain uses of data that are largely implicit in engaging in a transaction and shouldn’t require any sort of additional choice or I think particularly even an additional notice.

So, if you’re ordering a book, for example, should you have to be provided with notice that that book company is likely going to provide your address information to a separate company so that that book can be delivered? I don’t think you necessarily need to be given that notice. I think that’s implicit in ordering the book. There are different categories of those. I’m not sure that that information, when it’s provided, really helps any individual make a better choice in those instances. I just think it makes the notice a lot longer and read more like a large legal document.

Another one that I would state would be in the area of security. I’d be interested maybe in a show of hands. Is there anybody in the room who has read a privacy policy and read specifically the security section and said, now that I’ve read that, I really don’t want to provide the information to this? So, we’ve got a couple

people. I'm surprised because everything that I read says we provide reasonable and robust security. And I say, all right, I've been a lawyer for an IT organization for a long time and I'm not sure I know what that means. But c'est la vie. I think there's a bunch of categories we could take out of the notice.

MS. MITHAL: Okay. Commissioner Stoddart and then Fred?

COMMISSIONER STODDART: Yes. Just to remind us that there may be light at the end of the notice and choice tunnel because about 450 million consumers in the EU and 36 million in Canada have never used that model. we used informed consent. There doesn't seem to be the debate about notice and choice, I guess, because I think it forces us to be more simpler because the test is, does the citizen or the consumer really understand what they're getting into and really happening with the data?

So, I think rather than being viewed as a kind of notice of legal liability and what you will and will not do, it's does the consumer understand, and I think it forces the level of simplification. But I'm just presuming that.

I think it would be interesting to see what global companies that sell the same products in the United States and then in consent environments, how do

you change that particular part of linking up with the consumer and does that provide any ideas for innovative ways forward that are global?

MS. MITHAL: Fred?

MR. CATE: I was just afraid we were feeling too positively in here about notices by finding any proper uses for them, although I think the two last comments have helped to clarify that. I just think we should be frank. I mean, on the whole, notices have been an unmitigated disaster.

(Laughter.)

MS. MITHAL: How do you really feel, Fred?

MR. CATE: Look, I've toned that down for a public audience.

(Laughter.)

MR. CATE: And in many ways, I mean, not just because people can't read them or don't read them or all of those things, partly for reasons already touched on because they have become contracts. Therefore, any hope we had that they would communicate something intelligible, the FTC took away when it said, we're going to enforce these as promises that you will be held liable for. So, immediately we started adding the words "reasonable" and "where appropriate" and "as best possible" and we took what could have been a meaningful

notice and turned it into something that we would be able to fight about in court.

But in addition, notice has so often now become an excuse for not doing something else. We know we've got a problem, we were going to solve it. But, you know, let's just send you a notice instead, maybe breach notices being the classic example of that. So, we've lived through now seven years of millions of breach notices being mailed before finally a state got around to saying, you know, let's try to maybe stop these breaches, that would be an interesting idea, rather than wait until they occur and then send a notice and make ourselves feel better.

I think in fairness -- and I don't, in any way, want to get arrested before I get out of here or anything. But we don't just do this in privacy. I mean, there are many other examples of places, anyone who has ever applied for a home mortgage and gets all of the federally required notices, which, again, nobody has ever read and nobody will ever read or an informed consent notice in the hospital. It's something we use a lot in ways that are, frankly, inappropriate and becoming increasingly inappropriate.

So, while there are still some places notices can be used, I think we should be clear, at least, that

notices should not be the de facto position, and that when used in their other roles for transparency, for education and the like, we're going to have to move away from treating them the way we have treated them, if we have any hope of them ever conveying information that the public will care about or be able to internalize.

MS. MITHAL: Fred, if I could just stick with you for a minute. You talked at our first roundtable about the illusion of choice. And I think somebody here -- we started down the road of informed consent. But could you talk a little about what you meant by the illusion of choice and segue into a discussion of how we can actually make choice meaningful?

MR. CATE: Yes, I can, I hope. Let me just say here, too, because I don't want to do anything that makes it sound like I think choice is a good thing either, because, I think too often -- and again this has been well illustrated on this panel and earlier today -- we slough off good protection by saying, well, they checked a box. So, we should be very careful about not sort of celebrating choice in a way that's inappropriate.

But I think the illusion of choice is, for example, where we provided choice where there was nothing to choose from, so accept or decline, when decline shuts down the program, that's not meaningful choice in my

world. I don't think providing choice where the choices are, if you will, minuscule in comparison with the things people really worry about -- I often feel this way in the Gramm-Leach-Bliley environment where the types of things people really worry about with their financial information are not captured by the one choice that Gramm-Leach-Bliley gives us. You can opt out of certain marketing, sharing of information with third parties for marketing certain non-financially related products or services. It just missed the whole game. I mean, it's like arguing over the color of team uniforms or something instead of the playing of the actual game and how it comes out.

I think the illusion of choice is there when people either don't get the notice, so we say, well, I had a privacy notice, of course we know nobody has ever read it. That page has never been clicked on. But there was notice and, therefore, any choices based on that notice, particularly the default, where nobody changed the default because notice told them they would have to, that would seem like an illusory choice.

So, my basic principle would be any time where there is a choice that either is not real, there's nothing for them to choose from, or it's not about the types of concerns that would really face most consumers,

that is an example. I mean, we saw one quite recently, in fact, just the day before yesterday. I was flying in here and I saw a notice I had never seen before, which I'm just embarrassed about. But it said you do not have to provide this information to the TSA, but you will be denied boarding if you don't.

(Laughter.)

MR. CATE: Well, I'm sure somebody over there is celebrating that choice opportunity, but I would not call that meaningful choice.

MS. MITHAL: But just to follow up, is there -- I think you acknowledged at the outset that there is a role for notice when there's an opportunity for meaningful choice. So, where there are situations where there is an opportunity for meaningful choice, how can we implement that?

MR. CATE: Yes, and let me be clear, I do think there are places where there are meaningful choices. Particularly, just to take one example, where you're going to make a use of data that is unexpected and not related to the transaction, to say at that point, I'd like your permission before I do this. In that instance, I tend to think that just-in-time notice related to the choice almost always is the best way because people will forget about what it is they're choosing if you gave them

notice 30 seconds earlier or three days earlier, or heaven forbid, you know, three months earlier.

This, of course, makes a particular challenge for electronic devices that have to pose choices where they can't deliver the notice. So, you've got a hand-held device that may have a screen or no screen at all, or the computer in your car or what have you, where you had to make that choice in an earlier environment. You know, obviously, a very difficult situation.

So, I think given notice as contemporaneously as possible with the choice will help to make a choice more meaningful. Similarly, I think making the choice -- the notice as simple as possible and related to the choice. So, again, not notice about things which nobody would care or would expect otherwise.

So, for example, we have lengthy notices today about your information may be shared with service providers who will provide -- you know, the example of to mail your package to you, we're going to have to share it with the post office who may, in fact, share it with somebody else. But, instead, to focus the choices and, therefore, the notice on where you really have a meaningful choice to make.

And then I don't think it hurts to make that -- you know, maybe you have some other longer notice

available someplace else, but the actual notice at the point of choice to be really bold and clear and basic -- and I always describe these like cigarette pack warnings. If you can't fit it in a little box in 12-point type, it's probably too detailed for most people.

MS. MITHAL: Okay. Chris?

MR. HOOFNAGLE: I think the illusion of choice goes much deeper than just the notice problem. In particular, if you look at things like opting out of behavioral advertising or targeted advertising, you download an opt-out cookie. I think most consumers believe that that opt-out cookie means they're not tracked when, in fact, it means that they are not getting targeted advertisements. To me, that's the worst of all privacy worlds. You are still being tracked and you do not get the benefit of tracking.

We're now in a place where there are companies that are very powerful and are staffed by very smart people that keep reminding us that, you know, privacy is about the fact that you can tell them not to market to you about golf or tennis. But privacy, apparently, is not about the fact they have trackers on 70 to 80 percent of the websites on the Internet. So, your choice is, I think, completely illusory and counterproductive in a lot of contexts.

MS. MITHAL: Okay. Actually, that's a really good segue into a discussion on access. Chris, you mentioned the fact that companies may have data about you that they may not necessarily use. And I'm wondering if access is a way to address that issue so that a consumer might be able to see what information a company has about it. So, maybe, Paula, would you like to talk a little bit about access and the potential benefits of access, as well as some of the costs?

MS. BRUENING: Sure. I think access has a very important role when it comes to transparency. It informs individuals about what kind of data organizations have about them. It can promote accuracy of the data if there's a correction right, particularly if that data is really critical to some kind of decision making and it promotes the suitability of that data for whatever purpose that it might be put to. I think, moreover, it really enhances the trust relationship in good situations between the individual and an organization who is maintaining data about them.

I think, though, when we talk about access, I think we have to be careful about how we think about that because if you think about access as unmitigated right across all situations, I think you start running into problems pretty quickly. One is the cost issue. There

are legacy systems that have to be dealt with when you're talking about data. Data has to be collated from a variety of different places, some of them are quite far flung. So, making decisions about what kind of access to offer in different situations, I think, is part of this puzzle.

I think in situations where that data is really critical to decisions that are going to be made about me, I want to see the data itself, and wherever possible, I want to be able to correct that data when it's wrong. It's better for me, it's better for the company. It allows for a cleaner transaction. But when you're talking about large amounts of data that may be something like marketing data, it may be that to keep the cost down, but to maintain the transparency, we can provide a more generalized kind of access that says, this is the kind of data that we maintain about you. Now, you have a right, then, to suppress that data, to have us not act on it. There's another right that goes with that, but we're not in a position nor are we going to gather every single bit of data about you from every place that we might store it because that would be too burdensome. It's one way to approach it.

MS. MITHAL: Reactions, Richard?

MR. PURCELL: I have a concern about the

response that some companies make that say that it's just too hard to get to the data to give you access to it. Because, to me, that indicates that they don't know what they have, that they're not -- they don't have access to it themselves. And to me, my next question would be, are you over-collecting data? Because if you can't get to it, then why do you have it? How are you using it? Are you using it? And what is your retention policy? Because it may be that this -- the fact that I can't get to it or it's too expensive to bring it together means it's not got the value that you've promised me that it provided when you collected it under your disclosure.

It really does bug me. I have a feeling that the access discussion can easily reveal very poor information management practices, including particularly over-collection and over-retention of the data itself.

MS. MITHAL: John?

MR. VERDI: Just to echo what Richard said, there are also accuracy issues with that data because if a company is collecting data, using data and disclosing data that they've associated with an individual and then says to the individual, well, it's too hard for me to give you access to the data or to authenticate that you are who you say you are so that I can give the right

person access to that data, perhaps they ought not be disclosing that data to third parties and making a representation that it's about this particular person.

I mean, some of the basis for this data collection and these data disclosures is the company making the link between the individual and the data. Well, if they aren't terribly confident in the link and that comes out in the access and authentication process, that's sort of your answer right there.

MS. MITHAL: David?

MR. HOFFMAN: So, I have a long history of bugging Richard. So, I'll continue to do that when he said that this really bothers him. I would want to come back to the first thing that we talked about about the breadth of the scope of what personal data could be or personally identifiable information is. The broader you go in in scope, the more difficult it's going to be to determine who you should actually give access to, how are you going to authenticate and identify. This data may, in the future, relate to a specific individual, but are you actually forcing me now to actually do that comparison and relate it to an individual to figure out if it should go to that particular individual?

These are not, I think, just excuses that companies make not to give access. Sometimes they are,

I would agree. But not always. It's not always reasons that their retention limitations are unreasonable. For example, I've talked to companies that do make software that does security screening. For example, they have to collect IP addresses to do the kinds of security screening. The retention period for those might actually be very small, but it's continuous.

When you get an access request in, what's the universe, when do you stop deleting? These are really difficult situations, which is, I think, the only thing I can think away on access is I think it is a fantastic aspirational goal and I think people need to be able to try to give as much as they get. I think in many situations it's very difficult. In other situations, it could actually be harmful in a number of places to actually provide more access.

MS. MITHAL: If I could just follow up on that. Is there some low-hanging fruit on access? So, for example, it might be one thing to get access to data that Amazon has about you, about your prior product purchases and that sort of thing. But then how do you get access to data that a third party might have on you that's not consumer facing? So, I wonder if anybody wants to comment on that distinction. Actually, let me go with Paula first since she had her tent up.

MS. BRUENING: Well, I actually wanted to respond to a couple of the comments made about prior -- you know, I definitely agree that it should be getting easier to provide access rather than harder. I think the systems are such that we should be able to gather it more quickly and I think the data that's available in the ordinary course of business, we should be able to make that available to the consumer.

But I think the sort of distinction that I'm talking about in terms of access has to do with the use to which the data's being used. If the data has to do with my tax return, if it has to do with whether or not I get a loan, if it has to do with whether or not I can either buy or operate a car, I better have access to that data so that I know what's going on. If there's a problem, I want to be able to clear it up. I do think there are different kinds of data and they may warrant different levels of access. But it really has to do with how that data's being used and what the impact is going to be on the individual.

MS. MITHAL: Fred?

MR. CATE: Yeah, I mean, I think there are loads of examples of low-hanging fruit where access could be provided. I think one useful place to look, I'm not suggesting you adopt this model, but simply a place to

look, is the experience we have with other laws, for example, the Privacy Act of 1974 and FERPA, both of which talk about systems of records, so that you say, effectively, I'm obviously not merely oversimplifying, but also being incredibly inaccurate. But Chris will clear this up in a second. But, effectively, if you maintain records in such a way that you identify them or you locate or you pull data out of them on a person-by-person basis, providing access ought to be pretty simple because you've got it there. That's how you use them. That's quite different from saying you have to search every PC in your business to see if anyone has an e-mail that has this person's e-mail address in it.

So, it seems like we could start with some of those. In fact, there's been very good work done on the Privacy Act since the Privacy Act. The GAO did a report. There were certainly other reports done by privacy advocacy groups about ways of modernizing that definition, but still keeping it focused on some notion of a system of records or records where you have information that is stored in some appropriate way.

I would also say I don't want us to trivialize the security issue here because I think it's actually quite significant, and it gets more significant the more important or relevant or sensitive, or whatever we want

to say, the information are. So, when the Federal Trade Commission's own panel on online access and security effectively couldn't reach a conclusion on access, I think it was as much the security concern as it was the difficulty issue that drove that. So, although we've certainly come further. We can do things now that we couldn't have done eight years ago when that panel met. I don't think those concerns have been resolved yet

MS. MITHAL: Okay. I want to go back to something that Paula mentioned in terms of access and correction and suppression. I think, and correct me if I'm wrong, Paula, I don't want to put words in your mouth. But I think you suggested that for marketing data, there might be categories of information and there could be a suppression right, whereas for other categories of data, there might be a correction right.

I just wanted to see if there were any reactions to that. Are there areas where we would want to give consumers a correction right and how do we draw the line there? Richard?

MR. PURCELL: Well, it's vitally important that you give people correction rights in a variety of scenarios. But at the most fundamental, if there is a denial of a service or a removal of a service or, for some reason, some lessening of the relationship, based on

information, the individual has to have an access to the decision points that were made, upon which that decision was made, in order to review them and correct any flaws in them. This goes directly to the idea of saying, you know, you present your credit card and it's denied. Why? You've got to give access to somebody by saying we're not providing you a service based on this data. The individual has to have access to the data in a reasonable way, and reasonable means timely, prompt and effective in terms of being able to challenge or correct it, in order to make sure that the service is being denied based on a fair reason and not some unfair reason.

So, this is the concept of redress. We have to keep in mind that although there's been a lot of discussion over this day and the prior two roundtables, that people are discussing each of the elements of the Fair Information Practices principles as if they stood alone. They do not ever stand alone. Remedy or redress, access and redress are related. They're related to the notice; they're related to the choices; they're related to the accountability of the organization. None of these are first among equals. They are equal concepts that all have to proportionately build a regime of respect for personal information.

MS. MITHAL: Okay. Commissioner Stoddart?

COMMISSIONER STODDART: I was just reflecting why are we talking about access so much now? I'm the fish out of water here, right? I'm really not in my element. It sounds to me, if I may say so, that we're talking about access so much because the consumer is nervous or ill at ease and concerned about his or her information and how it is being handled. If I reflect on our own organization that regulates personal information and a law that's based on the fair information principles, as developed by the Canadian business community based on the OECD guidelines, the same guidelines on which you based your fair information principles.

So, there's a whole series, as Richard has just reminded us, of principles. And I think if there were more emphasis on proportionality, limiting collection, the use principle, not collecting information for which you do not really have a use, that there wouldn't perhaps be so much anxiety about access.

I mean, I look at our complaints. Sixty percent of our complaints are about collection use and disclosure of personal information. I don't remember that access is way up there, but I don't have the annual report in front of me. I don't know why Canadian consumers aren't so concerned about access. That being

said, access are some of our most difficult cases and we're preparing to go to federal court on an access case, but in a real, kind of live human situation access case. So, I just wanted to put that on the table, that if you have a whole framework that is applied principle by principle, it seems to me that that would lower the demand for access.

MS. MITHAL: I want to follow up on a point that Commissioner Stoddart just mentioned, which is the point of collection limitation. I think we've talked at this roundtable and at prior roundtables about the benefits of having a collection limitation. And I wonder if any of the panelists want to comment specifically on that. In fact, Chris, why don't I call on you? I know that this is an issue of interest to you.

MR. HOOFNAGLE: Sure, I'm happy to talk about it. In looking back at three roundtables, one of the most salient arguments I think we heard was the idea of having a regulatory system that only looked at use of information and did not put limits on collection. There were a number of organizations that said, let us collect what we want and just create rules around use. And I was interested in why none of the advocates kind of jumped on that. It seemed to me that if you didn't have collection limitations, it could open the door to all sorts of

pretty bad practices. Spyware would be legal under such an approach. You could collect information that self-regulatory groups have said that they will not collect, such as sensitive, personally identifiable health information.

And just as Richard just explained, that fair information practices are related to each other, I think collection limitation ends up being closely aligned with use limitations and implementation. In looking at the Privacy Act, if you have a situation were an entity is allowed to approve uses of personal information, they are going to run wild with that authority. I think the FTC has 16 routine uses of personal information under its privacy act implementation. So, it seems to me that you're opening your door to a lot of problems down the road with different uses, unless you have collection limitations on the front end.

The other issue you see in the Privacy Act is when data matching arose. Once you have a lot of data, it becomes kind of impossible for decision makers not to use that data for new matching purposes that probably would not be approved of at collection. So, I do think we do need to talk about both the procedure and substance of collection limitation in thinking through these issues. Because on the back end, you're going to see a

lot of uses that are nefarious or objectionable if you don't place some type of limit on the front end.

MS. MITHAL: John?

MR. VERDI: I think that that's particularly true, given how quickly the technology evolves and how iterative a lot of these products have become. You don't need to single out particular products, but you can see how, you know, a single technology product, like Facebook, right, looked like something two years ago and it looks very different to its users now in terms of how it uses data and how it does things like that.

You can see how Gmail started out as an email service and then integrated chat and then became really social with Buzz and did a lot of other things, and used consumers' data in very different ways. In a lot of circumstances, these uses weren't just not implemented at the time of collection, they didn't really even exist or weren't even contemplated at the time of collection.

So, I agree with Chris. The only real way to head that off is collection limitation and not use limitation because you fall into serious problems down the road when you encounter uses that consumers and companies never contemplated to begin with.

MS. MITHAL: Paula?

MS. BRUENING: I would just like to comment on

both of these comments. I think when you're talking about the use model that I believe that Chris is referring to, it does not take collection limitation off the table entirely. I mean, to my mind, as somebody who worked in the advocacy community for quite a while, it was, to our great consternation, that purpose limitation and collection limitation and use specification sort of got written out of the rules. I think that in some ways that use model brings them back into play. But it becomes the company's responsibility to be answerable for the amount of data that it's collecting and the kinds of protections it's putting in place around that data. It also, I think, implicates the decisions that are being made about how that data is being processed and used when it comes to new business models and new technologies.

So, it's not a free and clear, you know, we collect all of this information and then there's really no responsibility about it. There's an answerability that comes with that use and obligations model that says, you know, I have to be willing to say what I'm doing and have good processes and practices around what I'm doing with respect to the data that I collect. So, I think it's a little unfair to just sort of say that it doesn't factor in at all.

MS. MITHAL: Actually, if I can follow up on

the last couple of comments. So, let's say a company has implemented this collection limitation principle and only collects the amount of data necessary to effectuate the transaction. I think John's point is that there still could be unanticipated uses of that data. So, I guess my question for the panel is, I hesitate to use the term "notice and choice," but how can we get informed consent of consumers when the data is used in an unanticipated way down the line?

Okay, David and Richard?

MR. HOFFMAN: Yeah, let me take a stab at that. I keep coming back to Richard's comment, which I thought was very insightful, that it's very difficult to take any one of these individual fair information practices and drill down on it without relation to the other. When I think about this topic, I think about it under a header of data minimization. For me, that tends to mean the categories of collection limitation, use limitation and a retention limitation. Because your question talked about what about subsequent uses, I think that we also -- you can think about retention limitation as the -- one of the best ways to prevent additional issues that come from security breaches. If you have gotten rid of the data, then it's not subject to being breached in the future. And that's also true for the collection limitation.

I think, going backwards, the original concept that people were thinking 30 years ago about how this would handle is not a concept of necessarily what they would call notice, but there was a concept of purpose specification. There was a purpose for which the data was provided by the individual and that that was obvious, not just from some sort of notice that was provided, but from the context in which that was provided.

This is why I think, once again, that this is incredibly powerful, this use-based model that's been developed which is to come back to that concept and say, it's the context which the data is being provided that creates what that sort of purpose specification should be. If you're going to then do something, there are a number of uses and potentially transfers that are implicit within that purpose that you are providing the data. And then if you're going to have a subsequent use for that data, I think it's quite good there should have to be a very effective means for exercising choice on that.

I think we've run, though, into two additional difficulties, which I will point out. I don't have very good recommendations on how to solve them. I think one is when the data is not provided by the individual. So, how do you manage purpose specification if it's actually

-- let’s say there’s a social network that’s created which I think very well might be created soon enough, the people who hate David Hoffman and want to discriminate against him. That might be -- a lot of people are going to join that and share information within that. I might be very concerned about some of the uses of that data.

I think the separate category is organizations that are created where the actual purposes we might determine to be malicious, or the purpose itself is they say, our purpose is to collect data and sell it to whoever would like to buy it. What kind of rules do you apply there? I think then that creates a situation where we probably do need some normative rules laid on top of these fair information practices to say, where are some -- there are some pieces of behavior that we just believe are malicious and should not be allowed.

MS. MITHAL: Richard?

MR. PURCELL: I think it’s great to kind of harken back a little bit. Some of these first principles that we talked about -- Jennifer mentioned the OECD guidelines -- really do encapsulate this. We’ve been splitting hairs ever since and we kind of are splitting these things into finer and finer points until they become less and less meaningful in some ways.

The original access and redress concept was

wrapped up in something called individual participation and, in fact, consent was part of that, too. And it was a great high level concept. The individual must be involved and participate in this process. First of all, by being able to make an informed decision. We got notice out of that and notice turned into a corporate liability, cover my ass kind of situation, and it didn't actually do a lot to allow the individual to make an informed decision.

The choice mechanism was every time you want to use data in a certain way and it's an unanticipated or previously unexplained use -- the idea of individual participation is what Paula was talking about earlier -- you pop a question to the person and say, hey, we just had an idea, you gave us this, this, you know, some time ago, we could do this with it, what do you think? That's not so hard to do, but it definitely falls outside of our current conversation about what consent and choice means. It really does let the person participate.

Participation also includes, what do you have on me, what do you know about me, and how can I make sure that what you know is accurate in some way or another? So, this idea that these principles have been teased apart to the point where they become a bit more difficult to manage, could be, if not resolved, at least we could

start the conversation at a higher level and say, these ideas of individual participation and of organizational accountability, which pretty well take up a lot of these principles, could be perhaps elevated to a different level of discussion. Instead of these practices and these command and control kinds of things, we could start talking about what outcomes are we looking for here, from both sides.

MS. MITHAL: Okay. I'd like to read a question that we got from the audience. The panel seems to be focusing on information collected directly from the individual. What about a company that minimizes the data it collects from the individual, but appends third-party data which is not necessarily relevant to the original transaction?

COMMISSIONER STODDART: Well, was the individual whose minimal data was collected told that this would be done, that this was purpose, or one of the purposes of data collection?

MS. MITHAL: Assume it was.

COMMISSIONER STODDART: Well, then, if the individual had an informed consent, they knew that their information was going to be used for that purpose, I think that's --

UNIDENTIFIED MALE: And have access to look at

it?

COMMISSIONER STODDART: Yeah, that's fine. Yeah.

MS. MITHAL: And if it wasn't?

COMMISSIONER STODDART: If it wasn't, well, there's a huge problem in our country, it would be illegal. I think we had a recent example in one of our investigations where individuals were not aware of the amount of information that was being shared with third parties. I'm talking about our Facebook investigation this summer, and this is clearly in violation of Canadian law. They have to know -- well, there were a couple of issues. There was no data minimization, there was access to a whole suite of data just to run an application and individuals weren't clearly aware of that

MS. MITHAL: Chris?

MR. HOOFNAGLE: I've been talking about the privacy problems of enhancement for sometime. The idea that you can go to another company and buy information about your customers, independently of their interaction, I think, is problematic. Look at a case called Pineda versus Williams-Sonoma. This is a situation where a customer goes to a store and at check-out swipes her credit card and then is asked what is your zip code. I think a lot of us have -- we might have different

conceptions about what that meant. Some people if you ask them, they'll say, well, the store is doing demographic analysis to determine where they should place their next Williams-Sonoma. Other people might say, well, they need that zip code in order to do some type of anti-fraud practices like you do at the pay at the pump. But what the store was doing was using the credit card swipe plus the zip code to use a reverse directory in order to get the consumer's home address.

So, enhancement is squarely in the area where it's about getting personal information from a consumer without telling them and personal information that they probably would not provide if you asked. I think it's an area ripe for FTC intervention.

MS. MITHAL: Okay. Fred?

(Laughter.)

MR. CATE: I think this brings us back to Commissioner Stoddart's reference to proportionality and, once again, it's not an area where black and white clear lines help us or are terribly useful. For example, if information is going to repurposed or it's going to be combined with other information in a way that could constitute a clear demonstrable harm, however we want to define that, or in a way that puts the individual at risk in some way, I think you would want one level of

oversight of that, if you will, so whether that's explicit opt-in notice -- notice and choice or whether that's regulatory approval or whatever.

In the example Chris gave, I guess I would go back to sort of the Fair Credit Reporting Act model, you know, as long as the first mailing to that address said, you can opt out of receiving these mailings, I'm not sure that it really would make a lot of sense to first send a mailing to the address to ask for permission to send the second mailing to the address to make the offer that then the consumer can opt out of. So, it would just take a little bit of common sense, a little bit of measuring or quantifying risk of harm or injury to the individual that might suggest the type of response to the repurposing of data.

MS. MITHAL: Let me follow up on that and also a point that David made about the need for, in some circumstances, informed consent when data is repurposed. So, does this kind of consent or choice, would that include, well, we collected your information for this purpose, now we're going to use it for this purpose, and if you don't like it, you can't use our site or you can't use our service anymore. How would people view that?

Commissioner Stoddart?

COMMISSIONER STODDART: Well, I mean, again in

Canada, I think that's not allowed by the law. You can only collect information that a reasonable person would think is appropriate in the circumstances. These are not weird Canadian laws. These are based on the OECD principles that we all -- your country and mine signed on to. And you have to get informed consent, you have to give access, and you can't refuse to supply the service or the product on the basis that the person will not give you the information, unless the information is appropriate to your line of business and to your service, in that context.

So, there's kind of an in-built protection. You can't trade a good or a service against information, per se.

MS. MITHAL: Okay. And, again, once again to follow up on Fred's point about scaling the type of consent to the risk of harm, does it make a difference whether the repurposing or the unanticipated use is sharing with a third party versus an unanticipated internal use? Is that a useful distinction?

COMMISSIONER STODDART: Well, you know, in practice, people don't know about these things usually. I mean, it takes a very sophisticated regulator going on an audit or, you know, how do we know what the companies are doing with information inside, you know? So, you

know, I think in the debate, people have talked about time being wasted on debates that aren't fruitful. I think it's useful if we spend time on things that can reasonably happen.

And this whole issue of unanticipated reuse, or different use, brings up the question, well, how long are you keeping this information that you didn't anticipate? A week, two weeks, a month before? I mean, is it hanging around for years? We look at now, it seems to me, that most businesses have a continuous feed of information from the consumer, so that, you know, it seems to me that this is not really a use of information that is very credible to a regulator.

MS. MITHAL: Other reactions?

MR. HOOFNAGLE: It seems to me the first third-party distinction doesn't make sense anymore. I think it can contribute to integration. Say that you look at companies that have 1,000, 2,000 affiliates, especially in the financial services world, it doesn't make a lot of sense. We're seeing -- you know, information collection on the Internet is done by an increasingly smaller number of companies, and we benefit them by saying, well, if you share data with third parties, you're going to experience these privacy regulations. So, I think it might favor hegemonic actors and it is something we should probably

reexamine.

MS. MITHAL: Well, let me just use an example. So, let's say data is collected from the individual to buy books, and then later, the company develops a model where they say, okay, well, we can suggest books for you. So, there's no kind of sharing with any third parties there. Should we be treating that repurposing differently from, I guess, other types of repurposing?

MR. HOOFNAGLE: If that's directed to me, I would suggest that generally first party reuses have to be looked at more carefully than they are today because of how large these entities have become. It's not just repurposing. I think the conversation cannot end around, is this an appropriate use? You have to also look at retention, what choice in the matter individuals have about this. Civil service access and law enforcement access, I think, also plays into the equation.

MS. MITHAL: Okay. David?

MR. HOFFMAN: Yeah, I would want to agree with Chris on that and just add something on it. I think unanticipated use is extremely important for us to get a handle on whether it's first party or another party.

UNIDENTIFIED FEMALE: (Off microphone)

MR. HOFFMAN: I'm sorry. I think unanticipated use is something that's very important for us to get our

arms around, whether it's first or third party. I think there is an additional issue with transferring to other parties, but it's not necessarily around the unanticipated use. It's around the anticipated use, actually. I think that's around what are the structures that are being put in place to make sure that the commitments that the first party has made are actually being realized by the other party. I think this gets to all of the work that's now being done on accountability and how to drive that from just within an organization to make sure that all the vendors and all the other parties are making real on those commitments.

MS. MITHAL: Paula?

MS. BRUENING: Yeah, I would just add that part of this analysis really just has to be an analysis of the risk to the individual of exposure to some kind of harm, the risk -- and that can be not just financial or physical, but also what we're starting to talk about as societal harm, as to reputation. So, that should be part of the analysis, as well as what are the expectations of the individual and making some judicious choices about that, the expectation of the individual, but also the societal expectation. Because I think we've seen instances where a company will step beyond some envelope, to mix a metaphor, and there is a backlash. There's a

public backlash.

So, we generally will figure out as we go, when we've gone beyond the boundaries of what people will accept, and it's that risk analysis. Part of the risk analysis is figuring that out as a company goes along. Because I think that bright line of internal versus external doesn't really work. You can have data practices internally and you can do analytics internally that can be just as harmful as anything that might be going on outside of the company.

MS. MITHAL: Why don't we now turn to accountability which David just mentioned. So, let's say a company has policies in place, it's got collection limitation, it's got data retention, it's got just-in-time notice and choice. And then let's say that, you know, an opt-out doesn't work. It has all of this inaccurate information about consumers. Oops, they retained data accidentally. What are some internal mechanisms that companies can use to ensure accountability of these policies? Are there technical protocols that could underlie a system? Can technology help here? What are some other internal accountability ideas?

Paula?

MS. BRUENING: Sure. Well, I think this

morning we started to hear about some of those. I think what underpins accountability is the fact that a company has made the commitment to be accountable and that it's got these internal processes and procedures to ensure that it's going to meet its obligations with respect to data. Key to that is making sure that everybody understands what those obligations are.

So, there was a discussion this morning about data tagging, so that you can get clarity around what obligations match to what data. But I think that's only part of the equation, when you're talking about -- you know, the protections within a company. I think that Drummond Reed talked about the fact that you can tag the data, but it doesn't necessarily mean that the policies that go with that data are necessarily going to be followed.

So, it's important to also have an educated work force, some protocols that help you make good decisions about that data, some oversight within the company to make sure that whatever those decisions that are being made are actually giving you good privacy outcomes. But I think what's also important to remember is that an accountable organization is accountable even when that data is being processed by a third-party agent or vendor, when it's being shared with a business

partner. There's got to be due diligence on the part of the company that those obligations that go with the data, that they are understood and that also the recipient of the data is in a position where they can actually meet those obligations.

So, this is really -- and there's got to be some opening of the curtain. This isn't an interior monologue. You've got to have -- these processes and procedures have got to match up to some external criteria. So, it's an internal process, but there's got to be an openness to the outside for oversight and enforcement.

MS. MITHAL: Richard?

MR. PURCELL: Well, certainly, accountability has to be supported and implemented with administrative, operational and technical controls. If there's part of that formula missing, then you don't have -- you can't establish that accountability.

One of the contrasts I want to draw here is that when we talk about the accountable organization, we begin to contrast this with an earlier discussion around user control, and there is, again, this sense that there are these monolithic or unilateral kinds of silver bullets that are available to solve this, and user control is, oftentimes, put forward as one of those. But

although user control of personal information, your control over your own personal information, is important, it's not a reliable way to provide privacy protections. I don't know what user control would have helped the people who shopped at TJX stores when they lost all of their data to a hack. Nothing would have helped. No Spyware detector or intrusion detection on a user's basis would have helped.

So, an accountable organization needs to be matched as a control to individual user controls over personal information as well. That has to be collaborative because this really comes down to having an information sharing agreement between an individual and an organization. And the organization, in taking on that responsibility, has to be serious about it, use administrative controls, operational controls, technical controls in order to do so.

As an example, we talked earlier about the need to encrypt email that has personally identifiable information in it. Well, fine, but it's not done. It's not done on a user basis. It's not done on an organizational basis very often. Most data is sent in the clear using emails, even from corporations, although it's generally a policy or an aspirational policy to prevent spreadsheets to being attached and sent outside

of the organization and files to be carried around on laptops. But we all know that that's not how it works in the world.

We have a long way to go, not only to creating the accountable organization, but also to understanding what these controls really mean in a way that actually liberates the service delivery, in a way that gives us the promise that the information age is actually going to do us more good than harm.

MS. MITHAL: All right. David, last word on accountability?

MR. HOFFMAN: Yeah, I'm actually really excited about the potential that accountability has to deliver real privacy protections for individuals as we explore it more. Marty Abrams and Paula from the Center for Information Policy Leadership, I think, have been true visionaries on this of recognizing that there hasn't been a lot of detail and specifics about what does it mean to be an accountable organization, even though accountability has been one of the fair information practices for over 30 years.

And I think if you ask people from organizations, do you work for an accountable organization, they would say, absolutely, I do. And then if you drill down and you ask, okay, so you have a person

who's clearly in charge, you have clear, delegated authorities, you have adequate staffing, you have a training and awareness program, you have a documented issue management process, you have clear individual participation processes, it's all documented and you could provide it to me and I could read it and understand it, and very few of them, at this point I think, would say yes. I mean, leading companies would. A lot of companies would, in this room, probably would.

I think the good news is that people are starting to drill down on this now and try to define it. Folks in the industry, along with regulatory participation, are starting to explore it. I also think, you know, there's a lot of -- we have a lot of guides from other compliance operations that we can look to, financial reporting, environmental compliance. There's a lot of other reasons we need to run accountable organizations.

I want to say one of the things I'm most intrigued by, Accenture, I know, designed their entire processes around the seven standards of the federal sentencing guidelines. And when I found out about that, I thought, you know, that's perfect because what we really ought to be doing is running an accountable operation so we can clearly communicate it to our CEO and

our general counsel in line with other obligations that we have to be an accountable organization.

So, I can't say enough about how important I think this work is and to have regulatory participation in deciding what the definition of an accountable organization really is.

MS. MITHAL: Okay. I would like to circle back to a concept we talked about a few minutes ago. There seemed to be a fair amount of consensus on the panel that there is a role for informed consent here. We talked a little bit about just-in-time notices. What I wanted to follow up on is ask, is there a role for standardization of this process? In other words, is there a way we could take the burden off the consumer to try to digest many different kinds of just-in-time notices? Is there a role for standardization?

Commissioner?

COMMISSIONER STODDART: Informed consent does not mean, in my jurisdiction, a whole series of complicated notices. You are not informed and you cannot consent if you cannot understand, a reasonable person, not necessarily with a university education, whatever, cannot understand what they are consenting to. So, informed consent is inimical then with a whole series of explanations that most people will just glance over.

We know -- psychologists, for example, in Canada have shown that there's a natural tendency just to go on, you don't read this stuff. So, you're not really consenting and you haven't been informed about what you're doing.

So, at a minimum, it's about going back to plain language. What is really happening here? And who talked about something that could just be, you know, on a cigarette package? It was Fred, yeah. You know, saw it in the airport recently in France, cigarettes kill. Never seen that before. I don't know if it was the French approach or what.

(Laughter.)

COMMISSIONER STODDART: I haven't been, you know, looking at cigarette packages or something. But I thought, oh, boy, you know, that's clear.

MS. MITHAL: If I could just follow up. Isn't there a difference between cigarettes kill and privacy, which may vary from business model to business model and consumer preference to consumer preference? Does that create a complication here and how do we address that complication?

MR. PURCELL: It is complicated. I mean, technologies, not the technologies themselves so much, but the models that technologies are used to support

today can be extremely complex. A simple explanation is not going to be usable because it's going to hide more than it's going to reveal.

At the same time, we talked earlier about, you know, the concept of kind of little, middle, big. Okay? So, one of the things that notices today are used for, of course, is to cover liability as opposed to expose real decision making. It's entirely possible, if we help kind of lessen that liability burden, it's entirely possible to say, look, here's the best case-worst case scenario for this condition. You can have the little condition. Give me your email address. I'll give you these services through email. The worst case is, I don't know, that I'll spam you or something like that.

The middle case may be worse. The worst case may be -- one of the things that people don't understand and companies will not reveal is, what's the worst case condition of you giving me this information. And it would help people to make an informed decision if they understood better what could go wrong here? Frankly, we could lose your data and that could be bad. Now, we prevent that by implementing these procedures. It gives a context for the ability for an individual, a reasonable person, to make a decision. Isn't that the reason we're supposed to be giving notice, to have informed decision

making?

MS. MITHAL: Okay. Fred?

MR. CATE: I rarely disagree with Richard, but I think he's out of his mind.

(Laughter.)

MR. CATE: This will be like drug labeling. You'll read the 65 complications you could get from using this drug and we all know that people still go right ahead and take the drug anyway. So, I think we need to be extraordinarily cautious here frankly in, again, overvaluing the role of consent here to start with.

So, one possibility, and this may be a lousy possibility, but would be for the Commission to think about identifying a sort of default scenario, to say look, if this is what you're doing, you owe no further disclosure and there's no need for further consent. So, if you're only collecting data to complete the transaction and you're only going to retain it as necessary for that completion of that transaction, you don't owe the consumer anything else and you're going to use appropriate security. There's no consent there. There's no additional notice. There's no any -- I know I'm filling out the form, I don't need a pop-up notice saying you're filling out a form now.

You might remember that disastrous road we went

down with the first version of the HIPAA notice where we were going to get consent to use information provided for treatment. Like I was going to go in and tell my doctor something and then be shocked if my doctor actually relied on it in treating me. Calmer heads prevailed and we finally got that taken out.

But I think one thought would be to think about are there defaults, maybe multiple defaults in different scenarios, where the Commission could identify, through research or through a rule-making or whatever, a process of saying, look, this is what consumers rationally expect here, don't bother telling us about it if you're just doing what you already expect. That might also increase the pressure, if you will -- that's a slight stronger term than I would like here -- on data collectors to say, do I really want to do something else? Do I want to retain the data? In which case, I know have to do something else, I can just use the default.

MS. MITHAL: Commissioner Stoddart, I'm going to give you the last word on this. Was your tent up?

COMMISSIONER STODDART: Well, it was. When Fred said we're relying -- placing over-reliance on consent, he was partly right and partly wrong, if I can say. Just to get something going, yeah. We do have different kinds of consent and the example you were

talking about is implied consent. So, you know, it's not an elaborate, formal, highly logical process every time. But the basic principle is, yes, I agree, but it can be implied from your actions at the time that you're giving the information.

MS. MITHAL: Okay. We have about five minutes left on the panel. I would just like to wrap up with a question to all of the panelists and if you could take a minute or less to answer this question. The question is, now that we're at the end of our roundtable series, what should the Commission do next? So, let me just go down the line and start with Paula.

MS. BRUENING: I think that going forward the Commission should heed what it's probably been hearing for over the last three roundtables and not use notice and choice as the starting point for the discussion. I think that it's just becoming increasingly clear. That's not to say you don't look at fair information practices, because obviously you do.

But I think going forward, the exercise needs to be, how do you make fair information practices work in the world that we've just described today? How do you make them work in a really dynamic environment, where there's massive change, incredible amounts of data, less and less ability for the individual to exercise the kind

of control that might have been envisioned in the 1970s? But I think the frustration is always that the conversation keeps starting back at notice and choice when that isn't really the starting point anymore.

MS. MITHAL: Fred?

MR. CATE: Thank you. Commissioner Stoddart described, I think, good data protection as a whole framework, and I think that is a very important concept and one we might keep in mind when thinking about ways of moving forward. So, if I had to identify an objective here, it is to have organizations or individuals who collect and use data to feel appropriately the burden of what they are doing, so that we don't regard it as a costless activity to the organization, but it may impose very significant costs on individuals.

There are a lot of ways to do that. Law is, I think, part of that for helping the organization feel the cause. But I think the way not to do it is to shift all of the cost back to the individual by saying, let's just ask you for consent, and if you'll go along with it, we can do any damn thing we please.

MS. MITHAL: David?

MR. HOFFMAN: So, I agree with just about everything Paula and Fred said except when earlier he said that Richard is completely out of his mind, which he

may or may not be, but I don't necessarily agree with that right now.

I think what I would recommend is, I do like this idea of going back and looking at what are these sets of fair information practices and not going down the road that others have gone down, too, by saying, let's have really detailed regulations that we're going to write specifically about how to manage and impose these, but instead creating some ability for some interpretation and flexibility on the enforcement of those practices as we move forward.

I think your question about standards was a really good one earlier because I think then standards is an interesting phrase because, to the technology community, you say standards and we think international standards organization, technical standards sitting around roundtables for about three years before we agree on something that we can all agree to and that has great interoperability and increased functionality.

But I think if what we mean by standards is more best practices that we bring people together and define some recommendations about what the interpretation of those fair information practices should be that could inform really robust enforcement action, and that that practice then would include academics and industry and

advocacy groups and regulators, that then makes a lot of sense to me.

MS. MITHAL: Chris?

MR. HOOFNAGLE: So, I keep on saying look back at the 1996 report, where Beth Gibbon (phonetic) said, the FTC, no matter what it does, should create metrics for outcomes for its approaches. So, if it's self-regulation, create some metrics that you can review the outcomes. If it's legislation, create metrics.

One area where you have a metric is adoption of privacy policies. The Federal Trade Commission created an atmosphere that caused companies to very quickly adopt privacy policies in the 1990s. We went from 20 percent to almost 100 percent probably today. Now, the harder question is, how do you build substance into those policies? It seems to me that the market really isn't functioning to create substance, because competitors are not rewarded for privacy by design or for privacy enhancing technologies. In fact, there's a lot of free riders that claim they do things like anonymise their search logs, and they really don't. And their competitors are investing serious research and money into true anonymization and they are not rewarded for that.

It seems to me that the Federal Trade Commission could do a good thing for consumers and for

competition by beginning to police the free riders who are claiming to do things that really are kind of laughable upon deeper analysis.

MS. MITHAL: Richard?

MR. PURCELL: For me, without any disagreement from the prior comments, there's a balancing here that I think is important. And deferring to the fact that our hosts here are the Consumer Protection Bureau, this is not necessarily or unilaterally a consumer-based society. We're also citizens. We're also -- we have a certain amount of shared human dignity that is important to respect and try and figure out. It's not all about consumers or users or any of these euphemisms we have to describe people who are carbon-based life forms.

The other part of it is I believe that that should lead us to a little more cross-cultural sensitivity about what the whole world is like, not just what the idiosyncratic American approach is, that we have to begin to think a little more carefully not to go down the prideful kind of data as personal property consumer protection exclusively path of privacy protection, but expand that and accept the fact that the world has different concepts of that and different approaches and at least let those influence the inputs and our thinking on this.

MS. MITHAL: Commissioner?

COMMISSIONER STODDART: Well, I don't think it's up to me to tell you what to do next, but just from the outside looking in, the FTC is a world widely respected organization and there are a lot of hopes put in the FTC's initiative in the area of data protection. Because outside the United States, we're all affected now by products and technologies that kind of wash over us, sometimes independent of what our individual laws are. That's a huge challenge. So, we're looking for some action within the United States. I'll just refer you to Pamela Jones Harbour's comments. Those would be places to begin.

MS. MITHAL: John?

MR. VERDI: I think we're at a point in 2010 where the FTC does confront hard cases sometimes in the consumer protection context. But the Commission also, on occasion, confronts very straightforward cases, cases with straightforward violations, straightforward bad actors, and I would encourage effective enforcement on those cases.

What effective enforcement means to me, in this context, is a prompt response to consumer complaints about a business practice, decisive action on the part of the Commission, and penalties that are proportional to

the violations. And I think that that would go a long way moving forward in the straightforward cases to help consumers.

MS. MITHAL: Okay, thank you very much, and thanks to the panelists and thanks you to Katie Ratte and Katie Harrington-McBride who prepared for this panel. This was a great panel.

(Applause.)

CLOSING REMARKS BY JESSICA RICH

MS. MITHAL: And if you could just stay in your seats for a little while longer, we have Jessica Rich, who is the Deputy Director of the Bureau of Consumer Protection, and she's been a leader at this agency on privacy issues for the past ten years, and Jessica will deliver some closing remarks.

MS. RICH: Before I make some brief closing remarks, I just want to thank everyone who made this event happen. First, the excellent FTC staff that put together this event so quickly after our second roundtable. In particular, Loretta Garrison, Caty Harrington Mcbride, Naomi Lefkowitz, Monas Mohapatra, Katie Ratte, Michelle Rosenthal, Randy Fixman, Chris Olsen, Maneesha Mithal. So thank you.

And I want to thank all of the panelists here, the panelists and the audience for staying interested, staying here. Look, you're all still here. And helping ensure such a comprehensive and relevant and focused event in all three roundtables.

So, in closing, I'd like to just talk briefly about the next steps in this process and the issues that we're going to consider as we move forward. It's sort of hard to talk to all of you.

As you know, we've had three remarkable

roundtables full of ideas and observations. Some old, many new. Our panelists have included many of the nation's privacy leaders and many of other nations, too. I can't see Jennifer from here, but I know she's there. We have many thoughtful comments to read, and I want to remind everyone that the comment period stays open until April 14th. So, if you have some good points, especially after this great discussion, please send in your comments.

We have some really, really -- despite all these excellent suggestions for what we're going to do next, we have some really, really difficult issues to grapple with, as I think you know, and we get just how hard they are. And I thought I'd just count the ways, mention a few of the challenges and the tension we're dealing with as we work through these issues.

So, we want consumers to have greater control, recognizing that they really don't want to spend time reviewing privacy policies, even short ones. We want to distinguish between data uses that raise privacy concerns, truly raise privacy concerns, and those that really don't and are benign uses, recognizing that privacy preferences are likely to differ across different individuals and that hard lines may be very difficult to draw. We want to protect privacy without stifling

innovation in a marketplace that clearly has been using data, personal consumers' data to create products that many consumers like, products and services.

We want to accommodate the incredibly diverse business models and privacy concerns that exist today and that may be developed tomorrow. Online retailing, data brokering, mobile devices, social networking, cloud computing, behavioral advertising, online medical information, identity management, location-based services, just to name a few. We talked about more today than that. And we want a relatively simple framework so that everyone can understand the norms and the expectations. And we want to improve on the current privacy models while building on and not undermining the progress that has been made under those models, and supporting and not stopping the valuable privacy work that's underway right now.

We've been encouraged, for example, by the steps that industry has taken in response to our call for greater transparency and consumer control in behavioral advertising. I should add, you know, it's not done and you keep working on it. We need to see how it turns out, but we want that work to continue. We have ongoing projects and commitments with our international partners to coordinate enforcement and policy development, for

example, in APEC, which Commissioner Harbour, who spoke to us this morning, has led. These efforts can be a delicate process and we don't want to disturb them and pull out of them.

Despite the cleared shortcomings of privacy policies as a consumer tool, they've been instrumental in promoting accountability among businesses. Many of us remember, it wasn't long ago at all when there were no privacy policies and no commitments made about how information would be used. So, we want to preserve, somehow harness that accountability while figuring out a better way to communicate with consumers about the kinds of uses and the choices they have.

So, clearly, none of this is easy at all, but we think it's worth it. The discussion at these roundtables and especially the last comments that were just made have told us loud and clear that the dominant models really haven't kept pace with the wide range of business models and data practices that are in today's marketplace, which is evolving, you know, every day. So, we have a lot of work to do.

In terms of how we're going to get that work done, we intend to continue the collaborative process that we've launched with these roundtables. Given the challenges involved, we aren't about to just pop out a

new framework tomorrow. We've had these roundtables and now let's just like propose this new framework, fully formed and ready for implementation. Instead, we're going to take some time to think about what we've learned here. We're going to be reviewing the comments. And then, you know, we're going to get our thinking together and likely, as we've done in prior processes, we're going to put some thoughts out for public comment and get more input once we focus the issues a little more.

In the meantime, we may reach out to some of you, in particular, to ask you to elaborate on some of the comments you've made here or some of the points that have come out. We really continue to appreciate your help with this immensely challenging, but extremely important project. And we look forward to our continuing work together. So, thanks again for coming and we'll keep talking.

(Applause.)

(Panel 4 was concluded.)

(The roundtable was concluded.)

C E R T I F I C A T I O N O F R E P O R T E R

MATTER NUMBER: P095416
CASE TITLE: Privacy Roundtables
DATE: March 17, 2010

I HEREBY CERTIFY that the transcript contained herein is a full and accurate transcript of the notes taken by me at the hearing on the above cause before the FEDERAL TRADE COMMISSION to the best of my knowledge and belief.

DATED: MARCH 31, 2010

ROBIN BOGGESS

C E R T I F I C A T I O N O F P R O O F R E A D E R

I HEREBY CERTIFY that I proofread the transcript for accuracy in spelling, hyphenation, punctuation and format.

ELIZABETH M. FARRELL