UNITED STATES OF AMERICA

FEDERAL TRADE COMMISSION

THE BIG PICTURE

COMPREHENSIVE ONLINE DATA COLLECTION

Thursday, December 6, 2012

9:00 a.m. to 5:00 p.m.

United States Federal Trade Commission

Conference Center

600 New Jersey Avenue, Northwest

Washington, D.C. 20001

Reported and transcribed by:

Gervel A. Watts, CERT*D

TABLE OF CONTENTS

P R O C E E D I N G S

- - - - - - -

OPENING REMARKS

MR. LINCICUM: Good morning, everyone. We're going to go ahead and get started. I'm David Lincicum, an attorney here at the FTC's Division of Privacy and Identity Protection. I want to thank everyone for attending, either here in person or on our webcast. This is The Big Picture. It's our workshop on comprehensive online data collection. I'm very excited because we have a great set of panels here and excellent speakers. We can get started as soon as we can, but I just want to take care of a little housekeeping before we get started.

First, there is a little security blurb I need to read. Anyone who goes outside the building today, before you come back in, you are going to have to go through the X-ray again. So take that into account with timing and everything.

In the event of a fire or evacuation of the building, leave the building in an orderly fashion. You then head out the building and head over to Georgetown Law Center across the street. We want to be in the front sidewalk and look for someone checking in on all of the conference center folks.

In the event that it is safer to remain inside,

we will tell you where to go inside the building. If you spot any suspicious activity among this Motley crew, please do tell security. This event is going to be photographed, videotaped, webcasted, and recorded. By participating in this event you are agreeing that your image and anything you say or submit may be posted indefinitely at ftc.gov or otherwise publically available on social media sites.

Now that that's out of the way, let me also talk about how we're going to go about this. We are going to have the first remarks from Commissioner Brill and then a presentation by Professor Dan Wallach. Then we will have three panels. The first panel will be about kind of the current landscape of comprehensive online data collection and the benefits and the risks involved. Then we will have lunch and then a second panel on consumer choice and attitudes towards comprehensive online data collection.

Finally, we will have a panel on sort of the next steps for the industry and what policymakers can do in the future to preserve the benefits of the data collection while minimizing risks to consumers.

Throughout the day if you have any questions for any of the panelists, there are several ways you can submit questions. For those of you in the building, in

your folder you should have some question cards. Just write your question on there, raise your hand and someone will come by and pick it up and give it to the panelists.

Online, there are also several ways you can submit questions, on Twitter with MR. #ftcpriv on our FTC Facebook page or by sending an email to datacollection@ftc.gov. All of that should be on the webcast page.

So with that, let's begin. I would like to introduce you to Commissioner Julie Brill.

(Applause.)

COMMISSIONER BRILL: Good morning. It's really great to be here and it's also really nice -- which of these mics is on, this one? This is the mic. Okay.

It’s really great to be here. I see so many familiar faces. I've met with many of you over many different issues. I'm waving to people in the audience. It's almost like old home week here. It's great. Because we're being webcasted today I also want to say a special good morning and welcome to those of you who are participating via the Web.

I'm here to kick off this workshop which is designed to help us dive into issues surrounding comprehensive data collection. Before I do, I have to say a couple of thank yous.

First of all, I've got to thank the FTC staff who put so much effort into pulling this together. This workshop was organized by the agency's Division of Privacy and Identity Protection, spearheaded by David Lincicum, who was just speaking, who has really spent the better part of the past few months sparing no detail for today.

So thank you to David and thank you to DPIP for the organization today. I also have to -- where is Mike Zanis? There he is. I think we all -- maybe you more than me -- Mike Zanis, a special thank you, who did not purchase my $25 Starbucks drinks this morning, but helped me navigate the line so I could be here on time. So thank you, Mike.

What I'd like to do this morning is talk a bit about what prompted the agency to hold this workshop and then mention some of my thoughts about this issue, which I'm hopeful can become part of the discussion today.

Two years ago in December of 2010, the Commission issued, as many of you know, a preliminary report proposing a new privacy framework for business and policymakers. Our proposed framework was designed to balance consumers' needs to protect their privacy interest with the industry's need to innovate, which in part relies on collection and use of consumer's

information.

Now, when we proposed this new framework, we discussed the challenges consumers face in understanding the nature and extent of current commercial data practices and in exercising available choices.

Now, one of the data practices we discussed, among many others, was the capability of internet service providers to engage in deep packet inspection. To date, deep packet inspection, or DPI, has been used for purposes such as network management and Malware prevention.

Because deep packet inspection could also potentially be used to amass information about consumer's every move online, we requested comments on how to appropriately protect consumers from this potentially intrusive technology.

In particular, we posed the question of whether deep packet inspection warranted heightened restrictions or enhanced consent. The agency, not surprisingly, received a significant amount of input on this issue. Some consumer groups, the Center for Digital Democracy and U.S. PIRG, for instance, urged the Commission to oppose any use of deep packet inspection by network operators, other than network management, for instance.

Their view is that the profiling capability of

this technology severely threatens consumer privacy. The Center for Democracy and Technology singled out deep packet inspection because ISPs serve as the gateway to the rest of the internet, and thus, have the potential to conduct profound and comprehensive surveillance.

However, CDT believed that any other technology that could also capture a similarly comprehensive picture of a consumer's activities should be held to the same standard. Some industry commenters said that deep packet inspection is not the only technology that can track nearly all of user's online activity.

For example, we heard from Verizon that cookie-based technologies could collect the same, if not more, information than could be captured through deep packet inspection. The Internet Commerce Coalition argued that if deep packet inspection technology collects the same information as a behavioral advertising network, deep packet inspection should not warrant heightened restrictions.

The National Cable and Telecommunications Association believed it would be competitively unfair to hold deep packet inspection to a higher standard. Indeed, numerous technologies can capture large amounts of information about us online or on mobile devices as we go about our lives.

Deep packet inspection, social plug-ins, HTP cookies, web beacons, browser capabilities and operating system technologies all collect information about our many online and mobile activities.

After reviewing the many comments that we received on this issue, one thing became clear to us, we need to find out more about how to differentiate the data collection capabilities of different technologies or even whether any differentiation is appropriate, which brings us to today. We're here to learn more.

When the Commission issued the final privacy framework in March of 2012, we identified comprehensive data collection as one of the areas that required further study. We committed to hold a workshop before the end of the year and by gosh, I think we have made it.

During today's workshop, there are some questions that I will be thinking about as we listen to the presentations and discussions. Perhaps you'll find these questions useful as well, so I will offer them up to you as food for thought.

First, when we addressed data collection and use practices that weren't choice in our privacy report, we put forth the following guiding principle: choice is not required for collection and use of information that is consistent with the context of the transaction or the

company's relationship with the consumer.

Today, as we consider the entities that are engaging and comprehensive data collection, let’s consider whether these notions of the context of the transaction and the relationship with the consumer might serve as useful frames for thinking about different forms of comprehensive tracking.

Second, let's consider the transparency of data collection and use practices by entities with which the consumer has a relationship, but in some cases, with whom consumers generally do not interface. These are entities that run in the background on our online and in our mobile lives.

Would extensive data collection and use by such entities be consistent with the context of the transaction with the consumer? And if so, under what circumstances?

Some are entities that have historically not been collecting information about our activities online, other than for network management and other similar purposes. If they were to start to do so, how should they communicate this change in their practices to consumers?

Third, what should happen in the event consumers have inadequate competitive alternatives to

choose whether to use the services provided by these entities or in the event that they are locked into their current service in some way.

Fourth, let’s think about whether the different technologies used to correct information about the consumer result in substantively different levels of tracking. As we delve into the technologies that enable comprehensive tracking of our consumers, we'll talk today about ISPs, operating systems, browsers, ad networks, as well as some additional players in the data collect eco system. Do these technologies fall on a continuum in terms of their current or potential data collection activities or are there bright lines that might separate some from others?

A couple of other points to consider as we launch into these discussions, we know that comprehensive data collection allows for a greater personalization and for other benefits for consumers. We'll hear more about these important benefits as the day goes on. And we know there are many contexts in which this greater personalization is desirable. There may be other contexts in which it does not lead to desirable results.

In an interesting article that I'm sure many of you read, which appeared in this past Sunday's New York Times magazine section, Professor Jeffery Rosen of George

Washington University described two distinct profiles that he was able to create for himself online: Democratic Jeff and Republican Jeff.

Each of these distinct profiles experiences the online world in a very different way. Rosen noted that with comprehensive tracking that will soon be ubiquitous, moving from offline, to online, to mobile, to digital T.V., we will soon see such granular personalization that each individual's digital experience may essentially become one that is created for him or for her. Is this a good thing or is this a bad thing?

Rosen doesn’t really answer that question. I suspect that there are as many different answers to those questions as there are people in this room today. More interesting to me is the question of when this will begin. Rosen does answer this question, he quoted the founder of one of the leading data aggregators as saying that this kind of seamless, multi-faceted tracking will begin, "Once we figure out the privacy rules."

Moving to more fundamental and more concrete harms that form more directly in the FTC's wheelhouse, many of you have heard me speak before about my concerns regarding ubiquitous data collection and use. I'm concerned that the rich profiles being created about consumers can be used to harm them at work and in their

financial lives. I'm equally concerned that consumers are unaware of this data collection and use activity or the companies that engage in it.

So they have very little opportunity to exercise any current rights that they may have to opt out, for instance, or any rights that they may have to access or correct information about them. Paul Ohm, a professor at the University of Colorado at Boulder -- who, by the way, we are delighted is doing a stint here at the FTC and who will be moderating one of today's sessions later on -- has pointed out that the massive combination of facts that companies can gather through comprehensive tracking can lead to what he calls databases of ruin.

Databases that make it hard to conceal aspects about ourselves that we would rather not be brought out into the open and that can harm us with respect to employment, financial opportunities and our reputations.

So that's it for my food for thought to help us start off the day. Let's begin because we have a really great program ahead of us. First up is Dan Wallach, associate professor in the Department of Computer Science at Rice University in Houston, Texas. Professor Wallach will talk about the different technologies that are capable of comprehensive tracking and the type of

information each of these technologies is capable of collecting.

Professor Wallach is also the associate director of the National Science Foundation's A Center for -- and I hope I get this right -- Correct, Useable, Reliable, Auditable and Transparent Elections, more commonly known as ACCURATE. Did I get that right? I don't know where the "A" comes from.

MR. WALLACH: A Center.

COMMISSIONER BRILL: Ah, A Center for...okay. Thank you. His research involves computer security and has touched on issues, including web browsers and servers, peer-to-peer systems, Smart phones and voting machines. So I'm delighted to turn this over to Professor Wallach. Thank you very much.

(Applause.)

THE TECHNOLOGICAL LANDSCAPE OF COMPREHENSIVE DATA COLLECTION

MR. WALLACH: Thank you very much for having me here. For those of you who are on the webcast, you should switch to my slides, which are in pdf. It should be called Privacy 2012.pdf. As I am talking, for those of you who just have the video of me and don't have any idea what slide I'm on, I will hopefully say just enough to clue you in to what page I might be on. Meanwhile, I got to try to figure out how to make this thing full screen.

I'm going to be talking today about privacy and tracking on the internet. They charged me with explaining to you how these different technologies work and I'm going to try to do that in a relatively policy neutral way. My goal is to tell you how things work, not whether I think they're good or bad.

In order to give you a warm-up, I'm going to draw some analogies from the offline world. Since it's Christmas season, we're going to talk about some things we're all getting in our mail these days. This is just a selection of catalogs that arrived in a single day in our mailbox.

So if you look on the back of these catalogs, you'll see there are all sorts of interesting details.

So here is a zoom in on the back of one them and you'll see that it has a customer code, a media code, and a coupon code. All of these are just numbers that are printed that are personalized to me on this catalog. Of course, these numbers, if I buy something from this catalog and they ask me for that number, then they can connect me to that particular mailing. They can figure out whether I got the mailing letter and looked at it.

I'm going to call this a first-party identifier. This is a direct relationship between myself and a vendor. There are a lot of different identifiers that are used in our daily lives to connect us to the companies with which we do business. Your supermarket rewards card, for instance. When you scan that card, they know it's you, and in return for giving up a little bit of your privacy, you get a little bit of a savings on products in the supermarket.

Likewise, if you have your Macy's credit card, then necessarily, Macy's knows what you do with it. Gift cards are similar. If you look on many of your receipts that you went and bought your coffee from Starbucks in the morning or something, you'll often see a long number. That number is unique to you and that identifies a transaction between you and the vendor so if you go to return it later, they can find it in their database and

keep track of their inventory, et cetera.

Now, I say credit card numbers as well, but I put an asterisk because this really isn't a number between you and the vendor. There is some other company, your bank, that is in charge of this number. Nonetheless, many companies will use your credit numbers to track you and they will remember what you bought over time with that credit card number.

Of course, the trick is all these numbers map you to an entry in a database somewhere that can track your purchasing history and then they can turn around and target you with coupons or advertising or what have you.

It's important to point out that with enough aggregation, they can make some very powerful inferences. There was an article earlier this year in the New York Times that explained how Target, a large department store, was able to infer pregnancy based on certain purchases that people tend to make when they get pregnant. The article goes into nice detail about how some father got very angry that his daughter was being advertised to. He thought, well, she's not pregnant. And in fact, she hadn't told him yet.

So the ability to make these kind of inferences -- I think the lesson Target took was this was: don't be creepy. We can talk about whether that's necessary or

sufficient later.

Here's another ad that I got in the mail. If we look at this and we zoom in, we'll see that this particular Bed Bath and Beyond coupon has a really long number on a bar code. This is a unique number. That means that everyone that Bed Bath and Beyond ships out an ad to has a different number. It uniquely identifies me.

If I use this coupon, they know it was me, even if I'm paying cash. They'll still know it was me, even though it's my wife's name here, but they'll know that this specific coupon got used by this particular person. So in return for a $10 savings or something, you've giving up a little bit of privacy and helping them profile you.

Let's get away from first party and talk about something more complicated. I'm in the middle of refinancing my mortgage right now. Low interest rates, gotta love it. I got this curious letter in the mail. It says, "You've received this letter as a result of our relationship with the National Credit Bureaus. We were notified of your recent mortgage inquiry."

And later on it offers me the chance to opt out by writing to Experian.

What happened here? We're going to call this a third-party relationship. I went to my bank, J.P.

Morgan/Chase and J.P. Morgan/Chase did a credit check on me with Experian. Experian sold that information to a company I never heard of called Cendera Funding, who then sent me an offer saying we'd like to help you refinance too.

Now that I've talked about first-party versus third-party relationships, in this case, Cendera has a relationship with Experian and they learn something about me. I had never heard of them before, but nonetheless, they learned something about me and they were able to advertise to me. Let's talk about how first-party and third-party relationships work online.

First, let’s talk about first priority advertisements on the Web. This is a screen shot of the New York Times banner from a couple of days ago. You'll see there is an advertisement for Marc Jacobs. I have no idea who Marc Jacobs is. I think they sell something. I put up some of the html code from the New York Times website that displays this advertisement. I've used highlighting. I've used some color and underlining to point to some of the interesting parts here. The block of stuff on top says when you click on this link, you’re going to visit the New York Times again and then New York Times will do something for Marc Jacobs.

The bottom part of this says, "Please display

this image that's served up by a New York Times server. Now, I want to walk you through what happens when a user clicks on this link. The user's browser will go back to the New York Times server and it will request a file of this name adx/bin/adx_click.html with a bunch of other information that was on the previous slide.

Then the New York Times sends back a message that is HTTP 302. That's a redirect. That’s a way of saying, hey, browser, this page has moved somewhere else, please go there. And then the browser says right. Okay. Off to marcjacobs.com, and you'll see that now the user ends up at this Marc Jacobs website where you've gone. You might notice that the request to Marc Jacobs has this: "?utm_source=nyt."

So Marc Jacobs gets told that you were visiting them from the New York Times. There is a building relationship. Marc Jacobs paid the New York Times for this and this lets them count how many clicks came through.

So targeted advertising, there are a lot of different ways that first-party relationships where vendors who know things about you will customize ads to you. The simplest example is a search engine like Google. Here I've typed a name of a camera that I might buy because, you know, my camera from last year is

clearly insufficient. I need to have the latest and greatest. So I if type Nikon D800, the ads from Google, the first two links at the top of the page are from companies who are assuming that if I'm searching for a Nikon D800, I must want to buy one. And here is somebody offering it to me for the low, low price of only $2,679. Yay.

In this case, what does Google know about me? All they know is I've searched for it. The inference is if I've searched for it, maybe I want to buy it. And that's a gamble that these companies are willing to take. So they pay Google and they put this in front of me. Depending on the relationship, they might pay per view or they might pay per click.

There's another kind of user profiling. This is from when I log into Amazon and I scroll down to the bottom of my Amazon page. You'll see that Amazon is making some recommendations for things that I might want to buy. I recently purchased a Kindle for my dad. So they're offering me a two-year warranty and a power adaptor. Yay. Likewise, I've been buying cocktail-making supplies because I really dig cocktails. And they're saying, boy, maybe you'd like to have a nice measuring cup or perhaps, this wonderful strainer, so that way you don’t get ice in your cocktail. In the

middle, since I've used Amazon's app store for my Android phone, they're offering to sell me an app too.

What's going on here? I buy a lot of stuff from Amazon. I think many people in this room also buy a lot of stuff from Amazon. Yeah. Ed's nodding. No Amazon customers here?

(Laughter.)

MR. WALLACH: Yeah. Now the heads start nodding. So Amazon learns about you. They're trying to do the online equivalent of impulse buys. Given what we know about you, you might want to buy this. I'm sure many people in this room might or might not be looking to buy the same accessories and doodads I am. So you see that they've customized this for me. Well, how? Based on a lot of things that Amazon knows about me.

So where do vendors get information about the user? On the right side of this slide is a set of advertisements that Facebook generates for me. I use Facebook. That's how my family sees pictures of my daughter. That's how I get to argue with friends about T.V. shows that haven’t been on the air in two decades. You name it.

Facebook learns a lot about me in order to generate these surprisingly poorly targeted advertisements.

(Laughter.)

MR. WALLACH: So Facebook knows who I am. They know my education because I put in my college. They know who I'm married to because I say that I'm married to her on my Facebook page. They know what I post. They know what I like because I say, you know, I like Lyle Lovett; favorite musician of mine. So they can figure out that boy, if he likes Lyle Lovett, maybe he likes -- they can make all sorts of inferences, which they surprisingly don't.

Likewise, they can measure a lot of things about me. I mean, not Facebook, but Amazon measures what I buy. They might be able to visit websites that I visit. We'll get to that in a minute. They can take my IP address and learn where I am, which is typically accurate to the city you're in, if not better. Although it sometimes comic. I was in Germany for a conference and Facebook was suddenly advertising to me in German. Again, not very well targeted, since I've never once written a Facebook post in German. I might not understand German.

Anyway, Facebook -- in addition to things that I tell them directly, they can infer things. They can infer things based on my friends. If my friends like "X" I might like "X." Or my neighbors, et cetera.

So that all first-party information. What about third party? What about parties that are -- you know, there's me. There's the company I'm dealing with and then there's everybody else. What can everybody else learn in this game?

Let’s say I'm car shopping, so I visit autoblog.com, a popular car blog, and you see up at the top there is an advertisement for the all-new Nissan Altima. I put up the html code from the auto blog website and, again, you'll see there's two main pieces. The bracket (a) that says what happens when you click on the link and you'll see that it mentions three different things: doubleclick.net, atatwola.com, and finally choosenissan.com. We'll get into who these companies are and what goes back and forth in just a second.

Likewise, the image is served up by this other thing, tomdm.net. So that turns out to be related to double-click, and likewise, Atwola is related to America Online, who owns Auto Blog. Let me show you what happens when you click on this link because it’s a little bit more complicated than the New York Times example.

First, the browser will go to doubleclick.net, which with that whole big long string saying, "Please get this image." Or browser, please go visit this next page. Double-click sends back a read direct that says please go

back to atwola.com. So they're bouncing you back to a different url, but it's still part of the America Online family.

So Atwola gets to know that you clicked on the link, and finally, they will redirect you again to choose Nissan.com. All of this happens -- you know, the user just clicks on a link. All of these transactions happen without the user knowing, really. And finally, you end up at choosenissan. All of this happens just because you click on one link. This is reasonably common in the online advertising world.

So what's going on here? Why are all these bounces? This is all about measurement. Double-click gets to measure that you clicked and Atwola gets to measure that you clicked. All of that measurement, in turn, affects how the money moves for people paying for you clicking on that ad.

Let's talk a little bit more about how some of this tracking works. Also, I'm going to talk a little bit more about geolocation as well in the mobile case in particular. Let's go back to this paper example. Here is that same advertisement from Bed Bath & Beyond. Let's scroll down to the bottom of the app. You see there's this Yonanas Ice Cream Treat Maker. Oh, boy.

There's a two-dimensional bar code, sometimes

called a QR code. What happens if you scan that QR code? I'm going to use this as an example to explain how cookies work. Just for fun, we're going to use this as our example. If you decode that QR code with your phone, what it gives you is a url. The url in this case is bqt.co, which is a company called BeQRious. At least I assume that's how they pronounce their name. BeQRious is somebody that Bed Bath and Beyond apparently hired to produce this little QR code.

So what happens when you go to that link? This is the full response that you get from the BeQRious server to your browser. So I'm going to break this down into pieces, that way we can understand everything that's going on here. There are two broad sections of any web response. There is a set of http headers and then there is a body with html and JavaScript and all that.

In the header, this is where cookies happen. Lots of other things happen too, but the thing that we're interested in are the cookies. And then in the body, the JavaScript can also do some tracking behavior as well. First, let’s talk about the cookies. In this case -- so what is a cookie? A cookie is just a string of letter or digits stored, as a set of key value pairs, in your browser. So a website can set a cookie and then when you visit that website again, it'll send the cookie back to

them. Very simple.

So here's the particular cookie that BeQRious is in my browser. I don't know what unbq stands for, but it looks like an identifier that's unique to me. Notice the expiration date. This cookie will live in my browser for 10 years and then it will go away.

So anytime in the next 10 years, if I scan another BeQRious QR code, then they'll know that it was me. Or they'll know that it was the same person who clicked on the last one. They don’t have the words Dan Wallach, not necessarily, but they definitely know that this is the same browser that we saw last time.

They also have some JavaScript code that can do -- and JavaScript is a general-purpose computer programming language that your browser runs and they have -- so their JavaScript executes this function that they wrote, tracking, and then it has this long string, which is probably another unique identifier unique to me. I'd imagine if I visited them later I would get the same string again. Let's look at the code for this tracking function. I'm not expecting you all to be able to read JavaScript, but I would encourage you to have a look at the left column of names that you see here.

What they're doing is they're asking my browser -- QR codes are things that people typically scan with

their phones. Your phone generally knows where it is. The phone can measure its location with GPS. It can measure its location by looking at the base stations, which is less accurate, but more available. Or it could just Google and others do tricks by looking at the nearby Wi-Fi access points. There are several different ways that your phone can figure out where it is with different degrees of precision.

Well, this company, BeQRious, is asking for everything they can get, postal code, country code, region, county, city, street, street number, latitude, longitude, altitude, heading and speed. If it's there, they're trying to get it. They want it all. What do they do? They send it back. So it gets stored in a database somewhere.

Now, as it turns out, your phone will pop up a little message that says do you wish to give this information? Yes or no? To which I typically click "No." But some users will click "Yes" and then they will divulge all this information. If they click "No," then it all just comes up empty.

So why is BeQRious, and for that matter, why is every company doing this? So I copied this from BeQRious's website. What's their pitch? Their pitch is wouldn't you like to know how many users scan your codes?

And wouldn’t you like to know how many users do it more than once? Now you can. That's their pitch.

They also provide all sorts of metrics and detailed information to help you, the advertising manager for Bed Bath and Beyond, convince your boss that the money you spent on this advertising was worth it. They're providing metrics and details, and graphs, and charts and data to help their customer, Bed Bath and Beyond, understand the value of the advertising they purchased.

This is a big deal in the advertising world because in traditional T.V. or newspaper advertising, you don’t get these kinds of fine grain metrics. You put an advertisement in the print New York Times, you know something about who's going to look at it, but you don’t really necessarily know how they're going to respond. So the results -- this might be a familiar looking diagram -- I visit BeQRious by scanning it. They actually don’t serve up the content themselves. They redirect me to a company called net biscuits.

What they do is they actually serve up a webpage, which is a little picture and I can click on play and have a video of this helpful person, explaining how to use this kitchen gadget. So there are all these companies involved in dealing with a simple little QR

code that I scanned out of an advertisement. I used BeQRious just as an example, but really, this is how a lot of ad clicks work.

So cookies; everybody uses cookies. Every website you've ever visited is going to set a cookie. How do you associate meaning with these cookies? Well, it's easy to associate a cookie with where you saw an advertisement. It’s because, you know, you generate the cookie for where the advertisement went, so therefore, if you get it back, it's very clear you can do these kinds of tracking. It's harder to associate a cookie with your geolocation.

In the case of BeQRious, they ask for your geolocation; although, with IP geolocation, just by looking at your IP address, they might be able to figure out something about where you are. Just a footnote, from my own computer, I went to ip2location.com and they gave me a set of coordinates in downtown Houston and said you're here. So they were off by about eight miles.

So my IP address from my home computer, they were able to identify my location within about eight miles. That's reasonably -- that's neither outrageously wrong or outrageously correct. That's what you might expect. Now, it's harder to associate a cookie with a real role identity.

Regardless, websites can easily store the information they gather and aggregate it together. So even if a cookie is never attached to your name or your address, a cookie could still be associated with your behavior over time. You know, there is a cookie that the New York Times gives you, even if you're searching anonymously, they can figure out that this particular anonymous person has a habit of reading sports articles. Or this particular anonymous person has a habit of reading the travel articles. And then they could perhaps use that to target advertising.

So we heard mention this morning what are social widgets. That very same Choose Nissan website has this up in the corner. Apparently there are 159 people in the entire world who like Nissan. So Nissan is putting this up there.

Why are they doing this? There are different variations on social widgets. Some of them will name your friends. Your friend Bob like Nissan. And the theory is that might help -- well, if Bob likes Nissan, I'll go out and get one. I don’t know. These social widgets are a lot like those images. They have JavaScript or images that are served up by third parties that are displayed inside some website. That 159 likes from Facebook, that was generated by Facebook. There is

a little piece of JavaScript from Facebook running inside this Nissan website.

So what that means is that Facebook knows now that you visited Nissan. What they choose to do with that information, I'm not sure. But they're capturing -- that information is available to them to be captured and aggregated.

Likewise, there are something called web bugs or web beacons. So wired.com seems to be the king of this. They have 13 different web bugs when you visit their home page. There is a wonderful open sore -- not open sores -- but a freely available tool called Ghostery that I use, which blocks all of these things, but gives a list of them.

First off, what is a web bug? A web bug is typically a single pixel image. You know, a one-by-one pixel image that's transparent. And these will all be piled into a corner where you don’t see them. So when you visit wire.com, it will load an imagine from Google analytics and then it will load an image from Microsoft Atlas, from Omniture, from all these other little companies and every one of them gets a shot at putting a cookie and tracking you.

In fact, web bugs can perhaps even track you if you try to turn the cookies off. That's a more technical

discussion that I'm going to have right now, but all of these, they're effectively just like advertisement, except they're invisible. They can measure where you go and they can aggregate behavior about you. Not necessarily Dan Wallach, but whoever it was who went there also went there. And again, through that aggregation they can learn things about you and create a profile.

Even third-party payment services can learn a lot about you. So if I went to go and buy that camera, maybe I would go to B & H Photo in New York, which I like doing business with, and when I got to check out at B & H, they say well, you can give us your credit card number or you can buy with Google Wallet, or you can check out with Pay Pal.

So these are services that a lot of consumers, myself included, really like because I don’t have to give my credit card number to a vendor who I don’t trust. Several years ago I bought a little Bluetooth contraption and I bought it from whoever had the lowest price I could find. So I spent five dollars less for my little Bluetooth contraption. A couple of weeks later, there was a $500 fraudulent charge to my credit card from some company that sells cell phone equipment. I'm like, ah, hmm. So I had to get a new credit number and blah, blah,

blah, a real pain.

Whereas, if I could deal with a company like that indirectly, through a payment service like this, then there's no credit card number for them to steal. But in return for this extra user privacy, I give up a little something. Now Pay Pal or Google Wallet learns about who I'm doing business with and what I'm buying there. Google knows a lot about me for other reasons because, you know, they know what I'm searching for, et cetera.

So there's a tradeoff here. I'm getting a little bit better security against credit card fraud and in return, somebody is learning a little bit more and aggregating a little bit more about me. Once these companies have built up a user profile, which may or may not have your name, what can they do with that user profile? How can I monetize all this information I have about you?

Well, the user visits a website. The website wants to show an advertisement to you. Based on all of this information that's been collected, that profile of you, in some cases, is put up for auction. I've got an ad -- I've got the opportunity to display an ad to a user who has the following attributes: he likes cameras. He likes cars and he reads the New York Times. Maybe he's

rich. Go for it. Now I might be more attractive to a high-end car vendor rather than a low-end car vendor. Who knows?

Anyway, they actually have a little auction and this auction happens in the space of milliseconds. At the end, whoever wins the auction gets to display the ad to me. It's amazing. This article that just happened over the weekend in the New York Times Magazine, explains in lovely detail how this market works. There are a lot of players in the advertising market.

I love this diagram. This came out roughly two years ago, but it tells you just how fine grained this market is with lots of little companies selling all kinds of new services. This is a two-year old diagram. I'd love to have a more current one. If you have a more current version of this diagram, please call me. Okay. Anyway, for those of you online, you can look through this thing with a magnifying glass. It's just a fantastic little diagram.

All right. In the time that's left, I want to go over a handful of little tips, and tricks, and details and other little bits and pieces that are relevant to our discussion. First, what about your operating system vendor? What about the company that controls the phone or the computer operating system that you're using?

Well, the platform has a lot control over how people use it. Probably the most notable example is Apple, who very strictly regulates what is and is not allowed in the Apple app store.

There was a case, roughly two years ago, where they tried to crank down on what advertising was allowed to collect. Now, you could argue that this is a pro privacy thing. Apple was restricting an ad's ability to do analytics, but -- and this is a wonderful quote here -- "Ads don’t exist without analytics," says a mobile ad executive. You can’t measure it. Can't bill it. And of course, Apple is offering their own ad system, iAd as an alternative. So you could look at this in a lot of different ways.

This morning, the Commissioner mentioned ISPs. ISPs, or for that matter, your corporate IT department, controls your pipe from your phone or your computer to the internet. What can they do? Broadly speaking, they can do two different classes of surveillance. They could do passive surveillance, which goes by the name deep packet inspection. If your traffic is unencrypted, they can see it. And of course, your ISP knows exactly who you are and where you live because they have a business relationship with you.

ISPs have the ability to do logging to save

things which could be used for law enforcement or forensic purposes. To pick one example, a large oil company in Houston, which I won't name, stores every packet that goes over their internet gateway for a month.

Every single network packet on their entire internet gateway, for a significant sized oil company, they save it for one month. Now, why do they do this? Mostly for forensics purposes. That way if some machine is compromised, they can go back and figure out how and why. But you can imagine this being used for all kinds of other purposes. It's technically feasible to save a huge amount of data. Hard drives are big and cheap.

The other class of surveillance or the other class of ISP -- I'm going to use the term "active engagement." So this could include blacklisting. An ISP might blacklist a set of websites like, say Pirate Bay. We don't want you to go to Pirate Bay. Or they might blacklist an entire protocol like ViD Tard. There are examples of both. Perhaps, less invasive, many ISPs do what's called transparent proxy caching, which is a fancy way of saying, oh, you're asking for that imagine from other there. I have already got it saved. Here, I'll give you my copy. This is a performance optimization that many ISPs in companies used to save bandwidth. Completely legitimate and there's a lot of internet

infrastructure now to deal with this.

Many ISPs, particularly, college campuses do what's called traffic shaping. So you're a bandwidth hog and you're slowing it down for everybody. So we're going to slow you down so everybody else can go. Traffic shaping can be done in a relatively agnostic way. I don't care what you're doing, you're just generating a lot of packets, so I'm going to slow you down. Or it can be done in a more focused way. You know, you're allowed to send the packets to there, but not to there.

Many companies will do this trick where if you make an encrypted connection to some website, they actually terminate the encryption at the gateway and then re-encrypt it back to your browser. So they can observe all of your encrypted traffic. Now, that might sound invasive, but if you are the aforementioned, unmentioned large oil company, this is a way of monitoring what's going on. They see it as a way of protecting from security compromise. Again, you can see it for other issues.

In some cases, we've seen active engagement where somebody tries to attack a website. A particularly notable example was prerevolutionary -- and I mean like, the recent Arab Spring Revolution in Tunisia. The Tunisian Government was trying to get in between the

Tunisian people and Facebook because they were using Facebook for organizing and the Tunisian Government was trying to capture all the Facebook user names and passwords as a method of surveilling their populous.

Perhaps more famously, there was a now defunct company called NebuAd, and NebuAd had a relationship with Charter Communications, a cable company/ISP. And their deep packet inspection technology was sophisticated enough to be able to say oh, there's a website going by, I'm going to insert my own advertisement in it.

There's an ad appearing in the middle of a website that the website didn’t put there. There were lawsuits, et cetera. NebuAd went out of business. This was very controversial at the time. A student of mine who was in China was complaining that he saw this sort of thing happening with a variety of other websites. So maybe other companies are doing this elsewhere, if not in the U.S.

I'll talk briefly about click fraud. I'm a security guy. I should mention at least one security concern today. In the world of advertisement, fraud is a big deal. I can put up a website and put your advertisement on my website and generate fake views or fake clicks and I can make money from you, which is to say I can steal your money with fraudulent advertising

clicks or fraudulent adverting views.

First off, there is a whole side industry of companies to help a website accurate measure or to help people generate accurate measurements in the face of this sort of fraud. Generally speaking, there are two different kind of security mechanisms can rely on. Either browser behaviors that let them distinguish a real click from a fraudulent click. I'm not going to go into the details for time. The other trick people use are big data analytics on the server side.

One of my former grad students works in the relevant group in Google, and through liberal application of beer, I've been able to learn just enough of how they do it. The gist is that they collect -- they don’t pay right away. They instead collect a lot of data about all the clicks and then in bulk they can say this pattern looks fraudulent. This pattern looks legitimate. And that's a big part of their anti-fraud mechanism. But the details are all very hush-hush, secretive because Google were to publish how they did it, then the advertisers or the click fraudsters would adjust their behavior. So it's very much a leap frogging kind of situation.

There are a lot of technologies that are available today for users who wish to control back with their own privacy. I personally run Ad Block Plus, which

is all about deleting ads. Your browser just never loads them. And Ghostery is a tool that focuses just on these web bugs. They basically work by keeping a blacklist in your browser and your browser just won't go there at all. Not only does this have nice privacy protection for me, it also makes the Web go a whole lot faster, which is sort of a nice benefit if you're on a slow connection.

Something that I imagine we'll be talking about more later today is this new standard called Do Not Track, which is an optional message sent by your browser to each server saying please don't track me. What does that mean? Very good question.

There is a whole family of technologies to protect your privacy, TOR, perhaps being the most popular of them. It uses -- onion routing is a sophisticated cryptographic technique that allows you to route your traffic through multiple intermediate hops, such that the final destination doesn't know who you are and somebody in the middle doesn't know where you're going. It's very good at giving you privacy. It's particularly widely used by people inside places like China or Iran to get out without the great Firewall of China being able to tell where it's going.

I will briefly mention that in Europe, there are these new cookie rules that require users -- that

require websites to give notice to users of various kinds. I've included one of these notices at the bottom of the screen. You'll see that to most users that's just a collection of Greek letters that they don't understand. What is this thing? Get this out of my face.

Users are really very bad at understanding these messages. Yes, no, whatever. Go away. Leave me alone. There are regulatory -- there are regulatory teeth behind this, which is causing -- so if you visit European folks' websites, you'll see these things increasingly. I've linked to one website where you can learn more about the Euro cookie rules, but I'll point out a little bit of irony, if you want the user to be able to say no, don't set this or leave me alone, the way that you might remember that is you would send a cookie that says leave me alone.

So the very way that I might deny cookies requires a cookie in order to remember my preferences. There's some irony there because cookies are a general-purpose mechanism. They were invented at the very beginning of the web as a way of self-fixing the "stateless nature" of the http of the web protocol. This is the way that Amazon remembers that it's you.

When you add something to your shopping cart, well, as I go clicking around Amazon, I want Amazon that

it's me adding all these things to the shopping cart so that way in the end if I go to the shopping cart, it's got everything I buy. No cookies, no shopping cart.

These technologies like cookies are fundamental to the way all kinds of web systems work. You can't just ban cookies. It's crazy. What makes cookies a privacy concern is when they have a long lifetime, like that 10-year cook from BeQRious. When data associated with them is shared with third parties, like what Omniture is measuring about me when I visited wire, and particularly, if there is sensitive information that they're learning. Like, maybe I have a medical condition and I'm reading a website to learn about that medical condition. That's an inference that I don't necessarily want people to be able to make about me because I might consider that to be private.

A lot of my current research is focused on Smart phones, so I'll give a one slide pitch for this. Most phone apps use the Web inside of them. So there's this big convergence going on. A phone app and a web page are almost but not quite the same thing, but there are some interesting differences.

There are more complicated permissions going on. Your phone asks you for permission to do things that are sensitive. That's eventually going to happen on the

Web as well. Likewise, advertising in your phone uses many of the same mechanisms. I'm going to skip ahead and mention that all these extra permissions in the phone can lead to some surprising results.

For example, Path got in some hot water when they were uploading your address book, your entire contacts list to their server because they were a social network. Well, there's this wonderful quote from their CEO. How come you didn’t ask permission before you uploaded the user's address book?

He said, "This is currently the industry best practice and the App Store guidelines don’t specifically discuss it," as in nobody ever told us that this was bad, so what the heck. They got in a lot of hot water for this.

My last point, if you want to do some kind of regulation, then you should regulate behavior, not mechanism. Cookies are everywhere and there are all sorts of alternatives to cookies. If you regulate cookies out of existence, people will find equivalent and alternative mechanisms. To fit one example, your phone has what’s called an IMEI number. That's the unique number that identifies your phone to your carrier.

There are lots of other unique numbers in your phone as well. People can switch to using those. So if

you regulate based on mechanisms, technology people will find other mechanism. If instead you regulate information flows, you can talk about third party versus first-party information. You can talk about short versus long-term. You can talk about aggregation packaging and reselling, sensitivity, attribution, et cetera.

If you're going to regulate anything, that's how you want to phrase your regulations, but whatever you do, please don't ask the websites to other the user. That's just a losing strategy. Instead, come up with good defaults that people can implement that makes sense. And a big important question is this opt-in versus opt-out business.

Historical note, since I am totally over time, I don’t have much time to talk about this, but there has been a long effort to do the platform for privacy preferences and this largely failed because there no regulatory teeth behind it. Lori Cranor is in the room. Where did Lori go? I saw her walk in earlier. There she is. Hi, Lori.

Since I'm late on time, I'll just say read her blog piece that she wrote a couple of days ago. It’s assumed. Summing things up, I will say that as a general rule you should focus on being agnostic about technologies. You should instead talk about information

flow.

And oh, by the way, if you're careful about what you're doing, you might actually have some benefit to consumers in the offline world because all the same things, whether it's consumer profiling, credit rating, financial records, medical records, criminal records in the offline world, there isn't much difference -- the line between the offline and the online world is blurring very rapidly. Tracking is tracking, no matter how it's done. So you might as well be consistent about how you treat the whole business. Thank you very much.

(Applause.)

MR. LINCICUM: Thank you very much, Professor Wallach. That was fantastic. We are running little bit late, but I still want to have everybody have their 15 minutes for break. Let's see, it's about 10:10. Let's get back here at 10:25.

(Brief recess taken from
10:10 a.m. to 10:30 a.m.)

* * * * *

BENEFITS AND RISKS OF COMPREHENSIVE
DATA COLLECTION

MR. MAGEE: Let’s get started. Good morning everyone and welcome to our first panel of the day. This panel is going to focus on the data collection landscape and benefits and risks of comprehensive data collection, which we're defining as the collection of data by all or most of the consumer's online activities across multiple locations.

Our panelists this morning include Mike Altschul. He's the general counsel of CTIA, the Wireless Association; Professor Neil Richards from Washington University in St. Louis; Ashkan Soltani, who is a technologist and independent researcher and consultant.

Next to him we have Professor Howard Beales from George Washington University and then it's Markham Erickson, general counsel for the Internet Association, and Lee Tien, who is senior attorney at the Electronic Frontier Foundation. These six panelists bring a wealth of knowledge and experience to the discussion this morning and we very much appreciate their participation.

Before we begin, I just want to remind the audience that we are accepting questions if you want to ask something of the panel. You can fill out a note card that is in your materials and hand it to one of the FTC

staff. If you're watching the webcast, you can file a comment through Titter -- Twitter at MR. #ftcpriv, or you could use the FTC's Facebook page or send an email to datacollection@ftc.gov.

Well, let’s start our discussion this morning by building off what we heard from Professor Wallach and expand on the discussion of what the comprehensive data collection landscape looks like.

My first question is directed to Ashkan. Ashkan you've done some research on comprehensive tracking. Can you talk about some of your work and give some examples of business models involving comprehensive data collection?

MR. SOLTANI: Sure. One of the first caveats about comprehensive data is that a big misstating is that it's not all of the data we care about. So for example, on the web browsing activity, the images that are downloaded or the content that is public from websites, we really don’t care about the collection of that so much in that it's available to everyone.

Oftentimes it's the content of the communication, so this is the email that gets downloaded or content of information that gets posted to a website or the metadata associated with our activity on the web or mobile devices, which are things like location

information, information about like, your browsing history. This type of stuff that I think is of concern. So there is, on one hand, the issue of how much of information is collected, in terms of all of the content information and the metadata information.

The other concern in the coverage of the amount of information that's collected. So for example, some of my research in the past has shown that similar entities, for example, one entity can capture up to about 88 percent of all web browsing activity on the web. This is a 2009 No Privacy Report, where we found the combination of Google services, Google double-click ad words, ad sends and analytics, wouldn't literally cover something like 88 percent of the top 100 and something, or close to that of the top 400,000 websites we looked at. So it's one entity tracking your activity across multiple websites and multiple places. It's not just the Web, right.

So we find similar entities that have products that are in there. So again, not to give up on Google, but we have things like -- so they have search history, browsing history, mal-maps. Those obvious things. Those are web-based things, but they also have Android devices. They have the activity of their location information associated to your mobile device, your application usage,

in car supports, Google T.V., who sets up boxes, Google Wallet. So these are a variety of different touch points.

A lot of these services, for example, you can browse anomalously or pseudo-anonymously for them to at least identify the data. But a lot of these services require that you log in with an email address or an identifier, right. So the Google/Android environment does not support updating of apps or downloading on the App Store without a log in, right. So this is something that we should be concerned about. And it's not just Google; we have companies like Facebook as well that track all of your activity on Facebook. Dot.com, the website, the Apps used on Facebook, the messages that I send. So if I send a url to you, Peder, I did some research a few weeks ago demonstrating that, when I send the url, the content of that url is recorded by Facebook and then made available to the domain owner, right.

So that domain owner gets to know someone that is 37 in D.C. sent a url. So that information is made public. And then, again, in the mobile environment, Facebook also has a mobile app. So when you use an iPhone and you connect with Facebook, that mobile app gets to know what app you used and what type of activity.

So I think it's the multiple touch points and

converge across a variety of activities, even with, you know, light anonymous things such as browsing behavior or usage behavior that can be considered comprehensive. It's not just someone sniffing on your pipe in the DPI process. It's a lot of that data that may not be interesting.

MR. MAGEE: Thanks, Ashkan. So all these bits of information, where do they go? Are they all put together into a profile or how are they used? What do they show that's been collected?

MR. SOLTANI: So for each category it varies, but for browsing behavior or for -- a lot of the big players we see things like an aggregation of email content, browsing behavior, app usage to build a profile about you that is often used for advertisement, right. And we see this both from the online activity or things like Verizon Wireless, right.

So Verizon Wireless recently announced that they are monitoring, I think it was something like mobile usage information, including the addresses, information urls of the website you visit, location of your device, and uses of application in the future. To build a demographic and interest categories that will -- that include gender, age, sports fan, frequent diner, et cetera, in a way that's not personally identifiable, but

that remains to be seen.

This is for marketing purposes and we know a lot of the aggregation techniques are often ineffective. So one entity receives this information and then makes it available to marketers in a form of a report. Like, what are your demographics of people that use your site or sell advertising to that information.

It's not just, you know, we have -- I'm not familiar with them in the cable world, but we know these airport hot spots, they do the same type of thing. Your apps go through the Wi-Fi connection in an airport. A hot spot is often to do media metrics, right. There is a company called Gywire that does this, where you use a Wi-Fi hot spot if you don't have a VPN connection, your information is collected and often used for this type of purpose.

MS. MAGEE: Okay. Mike, I want to direct a question to you if I could. What types of information about consumers are particularly valuable to businesses?

MR. ALTSCHUL: Well, I just want to -- I'll answer that in a moment -- but to the extent the carriers are looking at -- and the person focus is, as one found, on the table, the carrier was the ISPs arguing us as well for a network management, network security. And the flip side of any discussion about privacy is data security.

Data is not secure from hackers, from data thieves and the like. We're not going to have any privacy.

The great benefit of personalization to consumers is the value to businesses. McKenzie, through the McKenzie Global Institute identify four or five advantages that come to businesses through this kind of, you know, clutching of the data.

First, it makes information visible that hasn't been visible. I think many of you may have seen how Google has allowed access to its search queries where one of the really innovative results of that is that they are able to predict where flu epidemics are about to break out. They can do it two or three weeks faster than the CDC and others waiting for Public Health Services to provide reports. The future of privacy policy on a paper they've just published. They have a similar example, looking at search queries, they've been able to identify drug interactions between pairs of drugs that people have put in search engines and queried and have been far more effective in identifying those kinds of problems. So making information visible is certainly one benefit.

Of course, more accurate performance information, as Ashkan mentioned, you know, an average high metrics, making sure that money is being spent in the most effective way to reach targeted audiences or

consumers. More precisely tailored products and services, this is the kind of discrimination of price is usually alike. All of us, as consumers, or the businesses we work for want, you know, more or less of a product that we need.

And in looking at this information, it's incredibly valuable to help develop new products and services. Having access to search queries and the kind of information people are looking for on the internet can be really, really effective feedback for businesses looking to better serve their customers.

MR. MAGEE: To build off that, obviously there are a lot of benefits to data collection, but is there an inclination or tendency for a business to over collect, to get as much as they can and try to figure out how to monetize or use it in whatever way later

MR. ALTSCHUL: Well, as Professor Wallach indicated in his remarks, the cost of storage has certainly made it possible to collect more information, but there are reasons, for instance, the forensics, that you would want to have that information available.

I know in our industry we see widely diverse practices to watch how long and how much data is collected, for example, for forensic purposes.

MR. MAGEE: By forensics, you mean?

MR. ALTSCHUL: Well, if there is a security that has been hacked or some kind of virus or malware to be able to identify and get information about the source and they hold the service provider, at their gateways, to better identify and prevent that kind of attack.

MR. MAGEE: Okay.

MR. BEALES: If I can just add, I think it's important to keep in mind, too, the benefit of the advertising-supported content, where the information is used to both measure the advertising and how many ads are actually being seen as essential for that market to operate our internet with an advertiser-supported business model. Some of that information is essential.

Targeting, in a survey I did a couple of years ago, roughly tripled the price that advertising commands, compared to run of network advertising. That's an important revenue stream to the people who are providing free advertiser-supported internet content.

MR. ERICKSON: I'd also make one other observation -- is this mic on?

I'd just make maybe a couple other observations off that. In terms of the conference of data collection, you know, in my experience, the collection of data itself is not what most concerns the consumers, or really from an internet company perspective, mass collection of data

isn’t the evil in and of itself, it's the uses of data itself and how they are used. And my observation has been that freeing up data and having more data is good. It allows us to make better decision, data-driven decisions. We want to make different decisions on things that haven’t been surfaced in the past, government information is made available and that's far better than the reverse, which is locking up data and having data that is not as accessible.

So I think we talk about comprehensive of data collection, we need to talk about the uses of that data collection. In terms of what types of data are valuable to internet companies, it really depends on the type of service that we're talking about. So for every different service, the data that they need to provide their services is going to be wildly different.

MR. TIEN: I’d just like to jump in here for a second.

MR. MAGEE: Sure.

MR. TIEN: Yeah, there are going to be some potential benefits to this kind of big data, but I think it's really important to keep in mind that one of the premises of this is almost -- well, what I consider is sort of an insidious ethic mess, which is that collecting data about people, on people, without their knowledge or

understanding of what is even being collected or who is collecting it is fundamentally different from say, taking chapter readings of the, you know, bird's crest or something like that.

The Target example, which everyone, I think knows, which Dan Wallach mentioned this morning, is a really nice example of how -- what seemed like really innocent facts. Your purchase of vitamin supplements and lotions and unscented tissues, to name three out of about 25 components of Target's pregnancy prediction, were able to allow someone that really shouldn't know whether you are pregnant to actually figure that out with a tremendous accuracy. And it's not a situation where a person volunteered that to someone or even directly bought necessarily any product about it. It's simply that we have so much data. It's because some people volunteered data about their pregnancy status as part of Target's baby shower registry and then combined with all of the other data, you are able to make hypotheses and test them on all of this data in order to be able to decode, essentially, that gee, there are patterns of our behavior that we, ourselves, are not aware of. That can be used to discern what most people would consider highly sensitive information.

When I talked, I used this example all the time

and they are flabbergasted to realize that it is possible, without ever, you know, it's not because you bought a pregnancy test kit. It's not because of any of these other thing, but it's just from really, really innocent things that you can make these kinds of generalizations.

What I want to suggest is that this is sort of the -- this is why when Paul talks about the database is ruined. It is much more now what are the facts that you intent to disclose to someone. It is not a question is how confidential that data is being kept. It is about the ability to make the screen interesting in PowerPoint. The flip side of that is going to be Google Blue or something like that. But I mean, the breach of the data is remarkable and the kinds of things that can be said about a person are profound and they are going to effect -- if an employer -- if Target can do this, they can sell that data to your employer. The government can use this data. There are all of these threats that come with the ability to sort of pierce the veil of facts and reveal very, very sensitive about you.

MR. MAGEE: I think Ashkan had a comment and then Mike.

MR. SOLTANI: Just to make two quick points, which is 1) I totally say it's the collection that is of

concern, right, to the degree we brought up the cyber security issue. If this data is collected, the likelihood for breach or secondary use is then presented, right. And to the lawyers in the room, you want to ask like, you know, an odd example would be that you would have the right to hang a piano over my head right now.

You might have that right, but it exposes me to some potential harm if it's not taken care of or it's not properly secured. With companies collecting this information, often without users knowing, that collection exposes them to some sort of breach. We saw this a few months ago with a company called Blue Toad that leaked one million device UDIDs and device names, which then can be used to link to other information about consumers. Blue Toad was an analytics company for the digital magazines for iPads.

To Howard's point, I absolutely agree that there is an ad-supported economy and there's quite a lot of value in that economy, but it is important to point out that, you know, some of the biggest players in this economy, like the little -- they didn’t start doing OBA until 2007, right. Prior to that it was contextual and search-based advertisement.

Even in the OBA type world, we have to differentiate between information that users voluntarily

known give and share and information that is passively or surreptitiously collected about them to infer things. I actually personally feel that we're in this kind of growing pains teenager area of behavioral advertising or tracking in that companies will find that it's actually better to engage a consumer and ask for high quality data about their interest or the things they're willing to share and leave the sensitive things on the table and not try to surreptitiously infer things.

We had these in the magazine days where if you wanted a free magazine, you would sign up for the things that you're interested in like automobiles and bicycles, for me, but maybe not dieting because I was sensitive to that. And I think we might return to that where the consumer is engaged and able to provide valuable information that makes the economy work without this creepy, over-collection and retention for long amounts of time for the things that they're sensitive to.

MR. ATSCHUL: The difficulty with saying that the problem is collection is that some of the information is collected for uses that are incredibly valuable. I mean, it's pattern analytics that has cut the credit card fraud rate by about half. It spots suspicious transactions that may be fraudulent. You got to collect the data in order to do that. You can't say it's creepy

that somebody knows what my credit card purchases were, but it's great that they stopped this fraudulent use of my credit card. Those are two sides of the same coin.

MR. SOLTANI: Right. But the third side of that coin -- if it's a three-sided coin -- well, we go to the dice, but you've collected the information and you use it for fraud detection or pattern detection and then you have this information around and you're like, wow, this information is all so valuable. Let me also use it for marketing purposes or secondary use or let me keep it around for a long amount of time, risking consumers to breach.

MR. BEALES: If there's a problem with the use, that's the problem.

MR. ALTSCHUL: Well --

MR. LINCICUM: One at a time, please.

MR. ALTSCHUL: But this gets to the point that Professor Wallach made. We really shouldn't fall in the trap of looking at particular technologies or techniques, but what's the higher level concern or practice was at an earlier workshop in this room on privacy where I learned that the original LOB that this catalog -- LOB got his start with mail order and selling his boots by going to the state of Maine's registry of everyone who had purchased a hunting license in Maine since 1908 and took

that list and sent a circular, advertising the best boot store for hunting. Very effective. Same thing we're talking about today, but it's the practice and the conduct, not the technology that we need to focus on.

MR. MAGEE: Well, we want to get everyone involved here. So let me ask a couple of questions here.

I'm going to ask Neil, in particular, but anyone else feel free to chime in here. Are there special concerns about -- let's focus on the comprehensive side of this -- as the collection becomes broader and looks at more things, is there something in particular about that that raises special concerns or risks to a consumer's privacy?

MR. RICHARDS: Definitely. I've been trying to keep quiet because the first question was benefits or not. I was sort of sitting on my hands. I think there are some benefits, but there are also some tremendous dangers that we just need to think through.

I think it's worth repeating the question we've asked. What is it about the collection of data about all or most of your activities, as you are all consumers, across multiple platforms that is potentially problematic?

We've talked a lot over the last decade about identity theft, which is one risk, but I don't want to

talk about that because I think we've talked about that enough. I think there are three particular dangers that we should focus on.

First of all, it's an idea that I call intellectual privacy. It's the idea that when we are reading, when we are thinking, when we are communicating with our friends, with our confidants, when we are making sense about the world using Google search engines, asking silly or potentially embarrassing or deeply political questions, that's different.

We should be particularly aware about any kinds of activities that threaten or that create incentives or deter people from exploring ideas, from reading freely, from thinking deeply, from not having that momentary hesitation. Should I look up on Google this funny bunion that I have on my bottom? I don’t think you can get bunions on your bottom, but anyway, you may be deterring -- I'll just remain seated.

You may be deterring people from asking questions that also have value. I think just as we care about freedom of speech, just as we are concerned about chilling effects, about people expressing their political and their social beliefs, so too should we be deeply concerned about what people are thinking, searching, reading, exploring that we don't want to deter them from

that. So that's the intellectual privacy.

The second danger here I think is that comprehensive data collection and massive profiling creates a transformative power change in the relationship between individual consumers and businesses. Information is power. More information is more power if we're concerned about things like unconscionability, like subliminal advertising, as we have been for 50 years. We should be concerned about changes we are making as a society in the power relationships between consumers and businesses.

So for example, it can be used -- if we're feeling particularly paranoid this morning -- for blackmail. If I know something about you, if I know about your medical conditions and know about your political views, I can blackmail you.

Now, most businesses aren't in the blackmail business. It's illegal, but a softer form of blackmail is persuasion. If I know what your preferences are, if I know what makes you tick, if I know what you might want to do, what you've been doing, if I can use big data to learn that you're pregnant before you know that you're pregnant -- which is potentially possible -- or to know something about you that you don't know about yourself, then you can sell people things they might not want to

buy. You can shape consumers preferences. This is tremendously powerful.

Now, I agree with the other panelists -- well, some of the other panelists that there are lots of good things here, but I think we need to focus on the transformative power relationship. The other thing that the power relationship could be used for is what social scientists call sorting, the grouping of consumers into particular categories. Mike used the "discrimination." Economists use the word "discrimination" differently from the way lawyers use discrimination. This power also allows gender or demographic or racial or ethnic or political segmentation and discrimination in ways that we might find distasteful, to say the least.

The third and final risk here, and I know this is focused on business and the private sector rather than government, but those techniques of surveillance are government and company neutral, right. Governments can use these technologies too.

Even if we're not concerned about government surveillance, the creation of these databases, of intellectual profiles, of highly granular consumer profiles with the ability to predict individual behavior and learn things about individual identifiable people is something that the government could be particularly

interested in, either as a marked participant in buying the databases or in law enforcement or just sort of generally having a look, depending which way reform goes and we have that power too, to just have a look and see. This gives the risk for concern for individuals versus state power. It increases the power of government as well.

MR. ALTSCHUL: But there are also benefits there in something as simple as traffic patterns from the various wireless apps that track pattern that have been used and have been very valuable in local governments, identifying and designing solutions to traffic problems. That kind of information just wasn’t as easily and readily available before.

MR. RICHARDS: Oh, absolutely. And I don’t mean to say that this stuff isn't useful or this stuff isn’t cool. That there aren't lots of useful life changing things that can be used from our digital revolution at large. But to collect -- and this goes back to Ashkan's point -- to collect information for one purpose is different from collecting information for all purposes.

Now, I suspect there are a lot of lawyers in this room, myself included, lawyers and doctors, as professionals, are very good at obtaining information

from their clients or patients that are deeply sensitive, private, potentially damaging information. And we need that information to flow clients and patients to doctors and lawyers so that they can treat disease, so that they can get them out of jail, so that they can advance their interest with the Federal Trade Commission.

Now, when a lawyer receives a confidence from a client, that information is used for a particular purpose for the client's benefit. It is not then used for marketing to the client to sell to other marketers, to third-party marketers. I think it is one thing to say we can collect information for a particular use, of course we can. But it's an entirely different thing to say that that information now belongs to the company and the company can use it for whatever it wants. I think the reason we have these rules is because there is a power and balance between lawyers and clients, but we don't use patients and accountants and priests and the people they work with. I think when we have that power and balance, our law, for hundreds of years has imposed fiduciary duties. I think what we're seeing is the emergence of what we should treat as an information fiduciary.

Google, who has that balance, I have to say, has been a fairly good fiduciary of personal data, has lots of information about us from search and from cross

platform activities. I think we need to ensure, as society across the world, that information that has that value, that has that power, that has that danger is treated appropriately so that we can use it for the good benefits, like disease prevention and traffic control, but that we're not using our traffic control information to allow law enforcement or marketers to follow us around in real time, sort of a video version of Google Street View to see exactly what is going on.

I think we need to think broadly because if you thought back 20 years, we said you're going to be carrying a device in your pocket that is more powerful than Captain Kirk's communicator --or maybe 30 years ago -- people would've laughed at you. How many of those devices are in our pockets right now or in our purses that are also phones -- they're not just phones, but they're also computers, they're also video cameras and still cameras?

I think we need to think broadly rather than case-by-case. Well, traffic safety is important, so we need to do that. You know, the flu is pretty bad. We want to save a couple of lives here. I think we need to look at the big picture so that we don't incrementally move toward a society that none of us, businesses or consumers, would have wanted in the first place.

MR. ALTSCHUL: You're exactly right.

MR. BEALES: The whole point here is you don't know about those benefits until you analyze the information you collected for another use. The information that lets you monitor the local traffic was collected because the cell phone company needed to know where people were in its network. It's put to another use that happens to be a valuable use. If there are bad uses, let's restrict those bad uses, but we've got to focus on the use because it's not a problem that there is less congestion on city streets because of information sharing. And if there are some sensitive categories of information like your doctor and lawyer example, I don’t think that's a power imbalance so much as it's the nature of the information that is being provided and the nature of the services that are being provided.

But it doesn't make sense to say that a department is a fiduciary, which is what you seem to be arguing. Let's not use that information for anything other than the purpose that it was collected for, which was to complete the transaction.

MR. SOLTANI: Why not a default rule, though? Just real quick, Why not allow people and incentivize people who could provide their information for traffic patterns and provide them with a rich incentive for

participating in that and allow the people that might have concern of secondaries to not, by default, be sucked up into the system.

I suspect in a lot of cases you might find, again, higher quality information for the people that are willing to participate and are actively -- I mean, we would have Neilson ratings for people voluntarily providing this information and they want to plan. They want an incentive to, right. We could have the same thing for traffic or for whatever else.

MR. BEALES: The difficulty with a default rule that is opt-in is that for most people the question of whether to allow the incidental use of where my cell phone is for traffic management is simply not worth thinking about. They have other things to do. There are actually experimental studies that indicate that the people who care more about privacy issues make consistent choices, whether the rule is opt-in or opt-out, but that people who don't care very much don't make consistent choices. The default controls.

If you care about privacy, fine, but it's not too much to say that you need to express that preference to someone as opposed to having us assume that your preference applies to everybody else.

MR. RICHARDS: I think the difficulty -- I

mean, returning from traffic to comprehensive online data collection is that most consumers don’t know what is going on. When they see the Facebook light button appearing on the New York Times webpage, they don’t know that if they are logged into their browser, which sometimes Facebook will sort of sneak that tick button in so that, you know, they want to certainly nudge people towards being logged in all the time so that Facebook knows that they're visiting that website.

Consumers do not know the level of the tracking. And when it's explained to them, they're shocked. I think it's entirely different to say we should have analytics that can monitor traffic congestion because you don’t have to have -- you can have anonymous traffic metrics.

They don’t need to know that it's me at the stop light, necessarily, in order to predict the traffic pattern. They can say that's cab. And that's absolutely fine. I think Howard is conflating very different kinds of data usage. With respect to the online stuff, I think what books you read, what searches you make of search engines, these are deeply, deeply sensitive kinds of information. I think if you were to ask consumers and people, as consumers, of course they don't want people to know what they've been reading or what they've been

asking or what they're wondering about.

I think difficulty is setting the defaults in ways that do take advantage of some of these potential benefits without saying everything goes, you know, if you're sort of one of those weird privacy freaks, you have to just opt-in, and honestly, we'll give -- so you have to opt out and we'll hide that opt out. It's in there somewhere in one of the addenda to the constantly changing privacy policies.

MR. LINCICUM: Well, let me ask a question kind of related to that then. You're talking about tracking books and reading and that sort of thing. Is there -- and I'm going to open this up to anyone who wants to answer it. Is there actually any commercial interest in that sort of tracking right now?

Is this something that is of interest to businesses in any way?

MR. BEALES: Well, Amazon clearly does it and consumers love it.

MR. LINCICUM: Context. A question of context, perhaps. Let me direct something over to Lee then. We talked a lot about breadth of information. Let's sort of combine the two subjects.

Is there any particular danger with combining, say a Facebook, who has a very deep set of information

about you that you largely volunteered, all about your likes and dislikes and connections with broader information from other sites, your Web behavior, the places you go, the places you search to buy, and combining those two kinds of information?

Does that present any special risks to consumers?

MR. TIEN: I don't think it presents special risks. It's simply a question of greater scale and greater magnitude. I mean, what we're seeing here is -- well, I guess the way I think about it is as information is stored, it will have a tendency to aggregate together. There are tremendous financial incentives to do that. There are known financial incentives to do that. It's a bit like in the second Terminator movie, I think, you blow that thing up, but all those bits of silver metal always comes back together again. I think it is almost an iron law, under our present situation that the data, without regulation, without some very strong technical siloing that the data that is collected about people is going to tend to aggregate together.

Obviously, Neil did a great job of sort of talking about brains and how we want to think about these kinds of privacy forums, but I think that -- what I wanted to add to that is, you know, he's absolutely right

that the ultimate question is sort of one of power and also one of fairness.

I think we tend sometimes to be looking for an example of individual harm or how an individual might be harmed as a result of something and at the same time, when we frame the benefit, we're often looking at these very sort of broad public good type benefits, which clearly could exist, but I mean, at the end of the day, to me, there is a threat model. The entities that have and can aggregate this data, they are not you. And your interest, the consumer's interest is not the thing that they are seeking to maximize in our system.

What we hope in our market-oriented system is that the brainwork, and that includes the laws and the regulations, will shape everyone's self-interest in a way that we actually come out collectively ahead. In a situation that we have right now where it's really obvious that consumers do not know what or how data is being collected about them, who is collecting that data, how it is being used, and what.

I'll keep back to this example, which is why I think that it's a folly to try to even separate the sensitive from nonsensitive data if they can figure out medical conditions from the things you buy at the store, then there is no way to say, oh, this is sensitive data

and this is not. It is all analyzable.

Plus, the scale at which you aggregate is simply one that allows for better and better mining and pattern recognition in these databases and that can be -- and if the incentives are not for the consumer, then they are going worth something else and those can be government surveillance. Those can be employer surveillance. There can be a whole lot of things that make it very, very difficult for individuals.

Now, the fact that technology changes all the time and it becoming so much more effective at both analyzing and inferencing with data collected, means that the democratic process in which -- to the extent that politics does reflect in some way what people know about a problem, how they understand it, and how they want to fix it, I think you'll end up with a political market failure there as well.

Frankly, one of the things that I worry about in this world of microtargeting is that is cause so much of electoral politics now beginning to have become much more tied to this kind of data gathering and political targeting to that.

It would be very difficult in a Washington, D.C. type environment to wean the political world away from the benefits of this. This is not just a question

of corporations benefitting from it, but politicians realizing that their ability to mine is something that they will value very much. I mean, I see some serious problems that we have with this.

MR. LINCICUM: I think that brings up another question and I'll direct this to Markham, initially, but obviously anyone can jump in afterwards. There have been some talk of maybe consumers not understanding what is going on. As far as you have seen, when companies are using sort of comprehensive data collection to innovate and create new services, how much are they thinking about their user's privacy when they're designing this?

Is this becoming a part of the design process as they develop the services or is it something that is thought about afterwards?

MR. ERICKSON: I think more and more the norm, especially with the bigger internet platforms, is internal privacy counsel and sometimes external privacy counsel are almost fully integrated with the product development so that the privacy considerations are being thought of at every stage of a service or a product being developed, and that's probably a good thing. I think, though, that the issue about the collection versus harm issue is an important one.

Ultimately, I think most of the examples that

we hear tend to be if this happens, this happens, this happens, and this happens, then this will be the harm.

So I think it's necessary for us to focus, in the policy space, about what harms we're seeking to address because that's ultimately where we land, in terms of talking about our concerns. It's what -- I think the collection itself, focusing on the collection itself is almost an impossible task to come up with the rule that just focuses on the collection itself because unless we're going to say that there is some sort of an inherent intellectual property right in persons -- in data, then there are jurisdictions that take more of a human right, intellectual right to the data itself.

I mean, in the United States we take more a tort-based approach, which is what harm will result from the use of data. I think that's a fundamental distinction that frequently gets conflated.

MR. BEALES: I just want to second that because I think the issue isn’t what consumers know. Consumers have no idea of what happens in the boot sequence when they turn on their computer, but they are reasonably confident it’s not going to blow up. They worry about why it takes so long. That irritates them. And they don't need to know. There's no reason for that information.

If you think consumers should be behaving differently, then you should persuade consumers to behave differently. That's what we do everywhere else. You shouldn't try to get the government to say you got to do it this way because it's the way we want to do it.

MR. ALTSCHUL: I need to chime in, second, third, fourth, whatever. Certainly, our associations, members, and we started representing service providers for that, broadly represent service providers an awful lot of wireless data services. They have incorporated the privacy by design concepts and they do have privacy policies that have adopted in this consumer best practices that consider the kinds of consents and notices.

While we'll be hearing from Gloria Kramer this afternoon, and I don't pretend to have the expertise that she and others have in terms of what consumers are understanding, in the marketplace, there certainly have been responses to these concerns, giving consumers far more choice than they had a year ago or two years ago. Just yesterday's New York Times had a story about wireless text messaging and the development of new alternatives for consumers like WhatsApp that doesn't present even contextual advertising for those consumers that prefer that kind of service.

In the browser world, Firefox has a very different kind of consumer experience than say, Chrome does or Internet Explorer. So we are seeing in the marketplace the development of choices and those choices must be based on the fact that consumers are interested in those services.

MR. TIEN: Can I jump in for three real quick points? The first is that obviously the collection constraints are not the only tool here that we have. I mean, one of the other tools is to simply discard and destroy the data once it has been used for the original purpose. You know, when we talk about Do Not Track, you know, in that discussion, we have been talking about well, you could allow longer retention or a long period of time of data in order to be able to deal with the click problem or something like that. But then at some point there will be a very clear, sort of distraction of the data. So there are ways, it's not just saying don't collect. It's much more than that.

Second, one of the distinctions that we have been using for a long time is the notion of volunteered, sort of consented to disclosure of data versus non. You asked earlier about how these things mix together, but one of the things that I worry about is that this distinction is going to sort of mater less and less

because of dynamic effects.

There is a professor, a colleague of Paul Ohm, who has got this understood, that has talked about the unraveling effect. And the unraveling effect on privacy is one in where it cause -- some consumers may have say, a very driving record, a very good credit scores or whatever, they have an incentive to disclose that in order to get some sort of a benefit. Then what happens is anyone who tries to maintain their privacy about a matter like that, there is automatically, say, a negative imprint.

Well, it's kind of like you're applying to school and the people with the good grades sent in their transcripts and everyone else doesn't. Well, obviously the fact that you didn’t submit your transcript means that you suck.

So what you end up with is a very powerful dynamic over time, where no matter how much you want to be able to not say something, there is a strong incentive to disclose.

So this sort of dynamic effect in the area of disclosure I think is going to sort of -- it changes the character, or at least you change the way we think about what is volunteered information because it is more volunteered under kind of a duress situation.

MR. MAGEE: We just got a question from the audience I wanted to ask and then I hope we can switch gears a little bit and talk about some specific technologies. The question from the audience is to Howard's boot up example. What if the operating system was installing Spyware as part of the boot process? Aren't there certain things that are so unexpected that they should be disclosed to the consumer?

MR. BEALES: No. You ought to make the operating system stop installing Spyware. I mean, this is isn't a notice problem. This is an installation of software that you didn't want. You ought to focus on the problem. The problem isn't that I didn't know and if in the boot sequence there is a growing string of texts over time that it tells me about the things somebody thought I should care about that are happening, somewhere in there if there's a line that says I'm installing software now that is going to wipe your hard drive, I don't think that disclosure solves the problem.

MR. SOLTANI: So that would be more a matter privacy by design to block that --

MR. BEALES: I mean more of a matter of enforcement.

MR. SOLTANI: I'm a little confused. So if it's not installed in the third-party software, if the

operating itself -- if I understand the question right -- if the operating system itself collects data much like Spyware in the case that it records your click stream and records all of your browsing activity, what's your response there?

I'm sorry. If that's okay. It's not third-party. The operating itself -- this is the function of the operating system itself, much like, say, a mobile device currently -- under Verizon, currently records your click stream activity location history, et cetera. What would be the appropriate standard there?

MR. BEALES: There is no point, as I think we heard this morning, in trying to have an onscreen disclosure that says here's what’s about to happen in a circumstance where there's nothing in the world you can do about it, except get a different operating system. That's the level at which that competition has to operate. The operating system is going to collect what information the operating system collects. I don't know what it's got on there.

In the normal operation of my computer, it's got all sorts of history files because I can find things when I lost them --

MR. SOLTANI: Sure.

MR. BEALES: -- which is a good thing. I don’t

know what information it's doing there. I don't want to know.

MR. SOLTANI: So if most of the operating systems in the marketplace collect and transmit that information and it's not disclosed to -- and there is no market differentiation between the different operating systems providers, what would be your recommendation on the outcome for that scenario?

MR. BEALES: What should --

MR. SOLTANI: How would you address the issue that your operating system collects and transmits the information, not just by virtue of needing to work, but actually for other purposes like in the case of Verizon?

MR. BEALES: That is a question which it can't only, at the end of the day, be resolved in the marketplace.

MR. SOLTANI: If the marketplace has failed, though, and there is no differentiation, then --

MR. BEALES: There is no failure in this marketplace. So there's no differentiation because there is no differentiation in consumer preferences.

MR. SOLTANI: Again, this is like a circular argument --

MR. BEALES: If there aren't not enough consumers to support, okay, the kind of technology that

you'd like, the kind of approach that you'd like, then it's not going to survive in the market. You can't buy three-wheel cars.

MR. MAGEE: We're going to get into a little bit more of the competition angle in our next panel. If we can just move forward, I know that we've got some other things that we need to cover. One thing I wanted to ask about is in the Commission's March privacy report, as Commissioner Brill pointed out this morning, we talked about some of the heightened privacy concerns associated with ISPs using deep packet inspection for marketing purposes.

Yesterday there was a press release about the new Verizon Selects program that Verizon Wireless is launching. It seems that under this program, Verizon will target advertising based on its data usage, including their web browsing and use of mobile apps. Sprint has a program that can also target ads based on consumer activities on their mobile devices. The question is how are we seeing comprehensive data collection playing out in a Smart phone context?

MR. ALTSCHUL: With respect to the new Verizon service, I'm at a unique disadvantage because ironically, our office has been the victim of a fire cable cut yesterday.

(Laughter.)

MR. ALTSCHUL: So I can speak, I hope authoritatively from second-hand knowledge -- yeah, from my phone. Actually, in our office, everybody was using their Smart phone hot spots to tether laptops to get to the internet. But this is a service, as I understand it, that is opt-in and, you know, it's a contextual kind of service that is very similar to the kind of search engine query information that is, you know, being done elsewhere in the ecosystem.

MR. LINCICUM: All right. Since we are a little tight for time, I'm going to move onto a couple of questions, but I do have one from Twitter that I want to ask real quick because I want to make sure the audience questions are getting answered.

This is about collecting again. This person wonders if anonymizing the data at collection would solve a lot of the concerns that are there. And if so, would current technology allow that? I'll just ask that to anyone who has something to say.

MR. RICHARDS: I would say that it would solve many of the concerns, but this is sort of Paul Pelham's workday. But maybe it is. But Paul has shown computer scientists that anonymity can be reconstructed, but certainly, you know, things you can do, things companies

can do to collect the information is a responsible, private and respecting way. I think it all can be good.

I was a little bewildered by Howard's computer analogy, but I agree deeply with what Mike said about privacy by design by the professionals, professionalization of privacy. Getting privacy questions in at the design stage rather than having privacy being sort of marketing denial thing or sort of waving of the hands and really not doing anything. Privacy, if it's meaningful and if it is brought into business practices, if it is brought into the decision, ideally, if there's even market competition on privacy, you know, these would all be good things. Anonymization, right, privacy by design, engineering privacy and embedding privacy is one of the things that can help.

Moreover, it's the sensitivity to those kinds of questions by engineers, by companies, by chief privacy officers that really can help get some of many, most, maybe all of the benefits of these kinds of technologies without creating a lot of these privacy risks and privacy harms.

MR. ALTSCHUL: We're seeing the market introducing more encrypted apps like with financial services and the like, and the enterprise area, use of virtual private networks is a very good way of providing

more secure communications. On top of that, with an encryption so that as the technologies and the services that evolve as people recognize the importance of securing the communication, securing the privacy of it, we're seeing these features and functions built in. At the same time, we're hearing from law enforcement, their frustrations of getting access to some of this content.

MR. SOLTANI: I want to just add, we want to be careful how you use the word "anonymous data." It's not kind of magic fairy dust that you sprinkle that sort of renders it harmless, but there have been a lot of examples of companies claiming that they had anonymous data -- first of all, I've personally been able to reidentify that data or that identifier to user social networks. There was an instance where I was able to take over people's Facebook and Twitter accounts using an anonymous identifier.

So to the degree that you are using that term, you want to make sure that's vetted in the computer sense of the word anonymous. And that will always be an evolving standard.

MR. TIEN: If I can jump in on that too. I mean, I think the identification/memorization is something that has to be part of the toolkit. I would never suggest that it is simply a panacea, for the

technical reasons that we already know about. In the area of online tracking, such as with Do Not Track, one of the big fights -- I won't say fight. One of the big discussions that we've had -- well, sometimes I'm more honest than other -- but the discussions we've had over how do you handle this conundrum of data perhaps being needed for security or for billing or for click fraud, while at the same time wanting to mitigate the privacy concerns has been through trying to figure out can we use some kind of unlinkability metric.

Can we say, you know, 1024 unlinkability or something, as a way to, you know, have buckets that do not resolve, you know, a really granular fashion, but at the same time, from a targeting perspective, you know, if your cookie -- I mean, we saw it in Dan's presentation, just how much highly persistent unique identification is being used to rule out both the offline and the online world. But if your cookie is something that states four preferences, gardening, air travel, Hawaii and language: English, you know, perhaps that can allow the advertising without ever actually compromising the identity of the individual the way that a 16-letter or number string would.

MR. LINCICUM: Thank you. We've going to move onto another kind of more specific topic. One of the

things that, as Commissioner Brill talked about, really what started the move towards this workshop is the discussion of DPI and why we definitely wanted to look at all other technologies in a broader question, I think DPI remains in a lot of people's minds, sort of the poster child for what comprehensive data collections means. It's sort of the big bad wolf of this area in a lot of people's minds.

So I want to spend just a couple of minutes talking about that. What exactly DPI used for and what can it see?

What are the limits of what it can see from users and what is it that it can actually get from a user's activities.

Ashkan, if you'd like to start. I'd like to hear from everybody.

MR. SOLTANI: So deep packet inspection is simply being about to examine not just the header info that is associated -- the header info of a packet is basically the routing information that describes who the envelope is to.

So you can imagine an envelope in the U.S. Mail system, that's the outside of the label. Deep packet inspection is looking inside the envelope for the content of that envelope. That's things like the information the

user submits, the content of their emails, the content of the websites, passwords, cookies, et cetera.

Depending on the technology used, there is different limitations, for example, unless my ISP has a deal with VeriSign or one of the other SSL providers, they are not able to decrypt my SSL traffic, the traffic that is encrypted using my browser's https capability.

Now, in a lot of corporations like, including, I think, the FTC here, they use a technology called Blue Coat. Blue Coat, as part of the set up process, your IT administrator installs the certificate onto your desktop or your laptop that allows that system to decrypt both http and https traffic. So they are able to look all conference of communications, passwords, emails, cookies, basically anything that flows on the wire that is not encrypted using a secondary client site technology.

Now, you can use things like VPN solutions to then tunnel through those DPIs. So if I go with a third party VPN provider and I use encryption -- start an encryption with my VPN provider, then the only thing that the ISP can see is just my connection to that. You can provide another data internal traffic, but I'm in the same boat with the VPN provider that I have to trust the VPN provider that they're not inspecting my traffic or looking at my data. The same goes for TOR, right. I

think I made an example of TOR is when lots of issues where people will sell malicious software TOR exit notes and monitor all of your traffic there.

There is a really good article by Bruce Snyder from a couple weeks ago. He made a talk -- I was at an RSA this past year -- about the return of feudalism, right, and this idea that we will now kind of need to trust certain entities over other entities, right. So at some point someone has got to carry my traffic and unless all of the websites I go to support https and my ISP and is not able to intercept that encryption, I am vulnerable to whoever is carrying my traffic. So you have to trust someone. You might trust the VPN provider. You might trust AT & T; you might trust your local ISP or whatever. I'm sorry.

The point I was going to make is ultimately, you still are exposed to somebody and you have to let somebody carry your traffic, otherwise, you can’t connect to the internet.

MR. ALTSCHUL: And the reality is that all of us have routinely used lots of different service providers. So, you know, at a workplace, we'll have one address and identity and service provider. On our wireless devices we'll have another one. At home, we'll have yet a third. Then direct any of those through VPN

or our apps, in different apps than intended. So routinely, all of us with Smart phones in this room have a choice of either a commercial light radio frequencies or the FCC's Wi-Fi network as a provider.

So the concept of a comprehensive one-stop shop to capture personal information from all the data that we send and receive is not accurate. These technologies and techniques, though, do have many of the same characteristics.

MR. SOLTANI: There was a case, as an example, with, I think it was publicly exposed with Sprint and their company called Carrier IQ, which was an analytics company that would monitor their traffic on the devices with for the purpose improving service. They were able to monitor their browsing habits, not just when you are on the Sprint network, but when you went home to your Wi-Fi and connect through your local Wi-Fi, they still would collect that information and provide that.

So I feel like, yes, to some degree, but again, at each step of the game, you either trusting your handset, you're trusting your ISP, you're trusting, you know, your keyboard or you're trusting your browser. At some point, each one of those entities has the ability to monitor your usage. And to the degree that you use something like single sign on, you know, either your

credit card, or your user name, your email address, any identifier that can then be linked to cross all of those different networks.

MR. RICHARDS: And when these stories break in the news and the information is made clear to consumers, the attention that these stories get, shows that consumers really do care about comprehensive tracking across the platforms.

MR. BEALES: I think the slides I have go to this question of the fragmentation of people's use of where they are online and how they are online. If this would be a good time to do those for 60 seconds.

MR. LINCICUM: Sure. If we can do that, yes.

MR. BEALES: I apologize to those on the webcast because these apparently aren't on the official slide deck. I'm in a business school and the number one thing we teach students is finding out ways to diversify to reduce your risk. And that's what's actually happening in the online marketplace, consumers using multiple devices, multiple networks, multiple browsers, from multiple locations and encryption is growing and all of these things reduce the extent of visibility into consumer behavior.

Multiple devices; this is data from 13 percent who own a laptop, a Smart phone, and a tablet. Obviously

the pair Y overlap is much higher. A 2010 survey that Pew did, the average person under 45 owns four internet capable devices or likely internet capable devices. All of those are used for browsing in different ways.

Consumers use multiple networks. This is sort of really striking, the extent to which people mix Wi-Fi and mobile access and how it differs across devices. Overall, 37 percent of the traffic from phones goes via Wi-Fi in this recent study, so even where it's going over different networks. People use multiple browsers. That’s not necessarily a choke point either. Browser market changes remarkably quickly. I picked 2010 and 2012 because it's the Commission's draft report in its final report. Internet Explorer market share fell 20 percent, and Chrome has doubled. This is the dynamic marketplace with lots of people using lots of different browsers and people browse from lots of different locations.

The chart on the left is NTIA data on where people browse. This is sort of a usual access kind of question. Forty percent home, 20 percent workplace, 9 percent coffee shops café. The chart on the right is a recent Google study that looks at the daily media interactions and asks how many of them were inside the home and how many were outside.

On a computer, 31 percent of the daily interactions are outside the home. On a phone, 40 percent of the daily interactions are outside the home. On a tablet, it's about 21 percent that are outside of the home. So there is this mix of home and not at home thing.

And, finally, encryption, it's not -- some very frequently trafficked sites, including Facebook and Google and Twitter, they have adopted encryption at various levels as part of the default for some of their services, in part, for security reasons, but it also means that it's a lot harder to read that traffic.

So I think there's not anybody with a single comprehensive view. The question is the extent to which you can make linkages across the different channels that consumers are using because consumers really diversified their risks.

MR. LINCICUM: Thank you. We have a question that was raised in the audience and I want to go ahead and --

MR. SOLTANI: I just had a quick question about the slides, which I couldn’t see them from here. I agree with everything on them, I'm sure. The question I had is in your examples, for example, different locations and different ISPs, how many of those consumers would use the

same common services like Facebook or Google to link on activity? Did you look at that at all or do you have any thoughts on --

MR. BEALES: I don't know. If you log into Facebook or Google, then you're going to be able to link across devices. That's clearly possible. You know, the thing about that kind of tracking is you can log out any time you want. The opt-out is right there and easy.

MR. SOLTANI: So some of research has shown that, in fact, you can't opt out anytime you want because sites will place persistent cookies, such as flash cookies, that prevent you from opting out.

Additionally, the flash cookies would allow you to link multiple browsers. So even when went from IE to Firefox and switched browser, they're the same persistent identifiers that would allow them to identify the same customer across multiple browsers, so perhaps not.

MR. BEALES: None of these are perfect separations. I'm not trying to say that. You can obviously make linkages, but there's nobody that's sitting on a choke point that everything goes through and that has a comprehensive picture of what's going on.

MR. ERICKSON: It seems to be a window data collections issue. But with regard to the questions about deep packet inspection, you know, the technology

itself is not a bad technology. It's used for a lot of good things, including to prevent cyber attacks and other things. The concern that's been raised by DPI is that it tends to be -- it's a server that tends to be at the endpoint of the network, so it does literally collect everything that's coming through the network. Again, that's just how it works, but it's the use of the DPI server that's raised the concern.

In the context of NebuAd, the concern was that because it can look at all the layers of the communication, in real time, I think NebuAd was advertising that they could send that to an advertiser and as you pulled up your web browser, you would get an ad that would be because of the content of that communication as it was being delivered live. There were a lot of concerns that would violate wiretap laws, among other things.

So again, I keep coming back to this collection issue, but the technology itself, I think we should be careful not to demonize the technology, but rather, again, going to the uses.

MR. BEALES: If I can just second that because it's one of the interesting ironies of controversy about deep packet inspection that the Commission's Microsoft case from 2002 on security issues specifically alleges

that among other things that were security deficiencies, was the failure to do deep packet inspection to protect the network.

MR. LINCICUM: All right. Let me get to that question we got from the audience because it is directed to this point you were making about fragmentation of people going to different providers throughout the day.

The question is, are the multiple options that you've described available throughout the U.S.? What about deeply rural America? Is there some constriction of the options available to folks, depending on where in the country you are?

MR. ALTSCHUL: I can speak to wireless networks. The Federal Communications Commission, as well as the CTI website has some very good data about the number of Americans with choices of five or more carriers, four or more carriers, three or more carriers, so that all but one or two percent probably the different one or two percent that are facing the fiscal cliff, but all but one or two percent of Americans do have choices of their wireless service provider.

MR. SOLTANI: Which I think is great. To echo Peder's point, two of the four major carriers are currently engaging in this type of collection. So you have two choices, and it’s unclear, actually. I know T-

Mobile does DPI for network management. They haven't announced their doing DPI for advertising and tracking. It would be fun to check in next year about this time and see of those four, if the other two are still engaged in those practices.

MR. RICHARDS: I think on the point about technology, DPI has some valid uses. It's like a gun, or a car, or a kitchen knife. You know, we can use them for good or for bad. But the important point is to focus on that is to be sure that you don't use -- just because DPI has good use, it doesn't mean that DPI is fine, let's use DPI for all things and for all purposes.

I think there may be targeted uses for some of these technologies, but it doesn't mean the technologies don't themselves contain risk. So we should be mindful about the power of those technologies, the same way we are mindful of the power of guns.

We don't get to bring guns into the FTC Conference Center. I guess I had to leave my outside. But we do like to have guns, regardless of one's politics, if for no other reason than we like having a military, and those folks have guns.

DPI is like that, right. It's one thing to say DPI can be used for network maintenance and security issues. It's quite another thing to say that DPI is sort

of a technology for all seasons.

MR. ALTSCHUL: I think somehow it's been demonized. The larger lesson, and I believe there is a consensus from all of us who have participated so far today that rather than look at a technology, you need to really look at the conduct and practices because cookies, the social platforms, the concerns that we all share in terms of protecting privacy go across technologies. By focusing on DPI or on cookies or on any other single choke point or technology, you really miss the complexity, the diversity and the importance on looking at identifying the conduct that you want to police and protect.

MR. LINCICUM: Well, I think that raises a good question. DPI clearly is a very powerful tool. It gives you a lot of insight into what -- or it can give a lot of insight into what a user is doing.

Are there other technologies that get you the same sort of insight and is there some way for us to put them on some sort of continuum or something to look at?

What is most invasive or useful that will tell us is it just an amount of information or is it the type of information? How do we look at this and decide what is most troubling?

MR. ERICKSON: I think from a policymaking

standpoint, trying to look at policy solution through the specific lens of a specific technology is always very problematic. Technologies change quickly. What DPI does now, some other technology may do in the future and I think it's been pretty successful in trying to avoid technology-specific solutions. So I think the exercise about looking at different technologies might be useful in some context, but trying to craft a solution based on that, I think is problematic.

MR. SOLTANI: I think I would agree. I think I completely agree that focusing on specific technology is actually not at all useful in this context. You can break it into the types of information -- I think Dan made a good point about looking at information flows, right.

Just to push back on Neil, some people would argue that DPI is not an okay technology. There's a school of thought, which is like the sanctity of the communication. The middle layer should be done and you can do most of the traffic shaping and network management features without unpacking the envelope. You can deliver mail without actually scanning inside the envelope. Some people feel that, especially with SSL. But with regards to out of other technologies or what information flows that technologies provide -- so at the core are your

monitor, your keyboard and your mouse have access to kind of all of your interactions, right, but except for keyloggers and stuff, we haven't really seen things looking at that information.

Then comes your operating system, right. Your operating system maybe uses multiple devices, but the operating system has visibility into all of your traffic, all of your activity, all of your behavior. And we've been pretty good in that regard.

We haven't seen operating systems, on the desktop side, collect too much user information, with the exception of like -- recently, there was some site called Ubuntu that would send a search history to Amazon and you would search based on the way they analyzed Amazon. And I think we'll see more of these as the operating systems move to move of a Cloud-based interaction, especially in the mobile arena, where mobile devices transmit information to the mobile carriers and the mobile operating system providers.

Beyond that there is the browsers, right, from the browser makers. They, again, have been pretty good about not capturing all of their traffic. Some will capture, you know, click stream history. Google has a feature that will sync your tabs across multiple devices so when you're on your tablet and your desktop, you can

see what tabs are open and read the same content, when, in fact, that tracks all of your present history, right, because it has to keep tabs of -- keep track of what tabs are open. No pun intended.

After the browser, comes browser plug-ins, right. Browser plug-ins, surprisingly -- Dan was making a really good point of Ad Block and Ghostery and such. These plug-ins have access to all of your traffic. Currently, we don't know of too many that are monitoring all of your data.

Ghostery is a good example where if you would able the ghostwrite feature, it will transmit all of your browsing histories. So every site you go to, it's a privacy preserving tool that will collect and transmit all of the sites you go to back to Ghostery. Not just the ones that have tracking pixels, but just every click stream.

It's important to know that these all have visibility into all of your traffic. If they wanted to, if they were malicious one day, they can actually capture everything you type or everything you read. Then you get into the ISP, which is this discussion about DPI, which the carrier itself can actually most of the traffic, except SSL. And in some cases they can view SSL.

And then finally, you get into this idea that

third parties that aren't on your device but are able to correlate your activity across your device, also have visibility, not just to your browsing history, but for example, I don't if you've used any of these copy and paste mechanisms where it lets you copy text off the New York Times and paste it in your email. They get that content that you've copied and they generate this unique url.

There have been some cases of more malicious ones that will scan the content of posts, but for the most part, the third party maintain visibility into your browsing history. I think the metric to the answer of how you carve it out, I think you carve it out in a simple way, which is like, low amounts of very sensitive information or high amounts, potentially, of that sensitive information that covers a wide portion of your life. This is kind of like touching on U.S. versus Jones, which is like, you can say it's either invasive or the aggregation of a lot of different touch points about a person's activity can also be considered kind of invasive. I don’t think there's a clear standard there, but I think that's the two axes that we're looking at.

MR. TIEN: Just to amplify that, I mean, at the end of the day, I don't think it's a matter of what the on ramps are. The question is however fragmented or

vulcanized the collection might be, the product is data about the person and the person's activities. And thus, the questions is where does that data go.

If you believe in sort of the Terminator approach, then that data is going to flow someplace and become more centralized. So at the end of the day, I think it's much more -- while it is important to understand the size of the attack surface than what Ashkan has described is a very, very large attack surface. The big part of the question is, are we going to allow all that data to simply aggregate regardless of whether it’s coming from one point, two points, or 29 points. I mean, if it's all aggregating somewhere and then being used with no restrictions then we have a problem.

MR. MAGEE: The question I have now -- and this goes back to what Commissioner Brill mentioned this morning -- but in the Commission's privacy report -- and private, it goes back to our online behavioral advertising principles. We've drawn a distinction between first-party interactions and third-party interactions. We've said that with respect to marketing. In most cases, first-party marketing is somewhat transparent and intuitive to the consumer.

We made a distinction where the data collection

that's being used for marketing is happening behind the scenes by a third party that a consumer might not be aware of. We said where its first party, the collection and marketing is typically going to be part of the context of the consumer's interaction with the business of the relationship.

The questions is does that sort of paradigm work when we're talking about comprehensive data collection? For example, to go back to the ISP/DPI context, I have a relationship with my ISP for them to give me broadband service. As part of that, is it consistent with my interaction with that ISP that they're going to track me across websites?

Anyone can weigh in.

MR. BEALES: Let me weigh in first on the consequence because the tracking across websites is going to lead to an advertisement. It’s certainly consistent with your subscription to the Washington Post that they're going to market to you. The marketing is very much part of that relationship. That relationship uses information about the nature of the Post subscribers.

So I don't know what’s different about the subscription relationship with an ISP and the subscription relationship with a magazine or a newspaper that is going to give you advertising.

MR. MAGEE: Well, from what we've heard today, comparing what the newspaper would know about me based on, I assume my address, and what an ISP can know about what I do online. I'm not sure they match up too well.

MR. BEALES: But that is saying that the harm itself is knowing. And I don't think that's a defensible proposition. The harm has to be some consequence of how that information is used. And if the only use you're worried about is marketing, well, you know, that happens all the time and consumers expect it.

MR. ALTSCHUL: Well, to the extent that consumers don't like it -- and we've seen this with some of the changes, in terms of service on Facebook and other sites -- they let their views be known very, very quickly. So we've come a long way in the last few years in terms of sophistication, not just as industry professionals but as users. Of course, the norm continues to evolve along with the technology and all of our experiences.

When some of these applications and uses get ahead of the norm, there is a lot of pushback, which is a good thing.

MR. TIEN: I guess I don't quite get the analogy because I think that -- well, certainly, when the

DPI issue first came up, a lot of people that I talked to and when I talk about it, it's sort of like, yeah, this is like the phone company listening to my phone calls which is something that the average user of phone service simply doesn't expect.

I mean, the idea of in that relationship is that they are acting pretty much as a conduit and not paying attention to the content of those things without some exceptional reason.

We have norms, the legal rules under the Wiretap Act that make it very, very clear that the role of that kind of service provider is not to acquire content without very, very specific authorization. So I think that that's very different from say, subscribing to a magazine or a newspaper, where you are receiving content from them in sort of the traditional advertising stuff. I do not really see the analogy there.

MR. SOLTANI: I think it's a -- sorry. Go ahead.

MR. RICHARDS: I was going to say that one of the difficulties on focusing on context is if we're talking about all these new exciting services. We don't really have -- or one could argue, we don't have a context, other than the way things are. If the context becomes the way things are, then context is not providing

any check on the ability of this kind of activity to occur.

If we're talking not reading, I mean, we have context of reading, right. When you read a -- not that we do very much anymore -- but our social contexts are about paper newspapers, right. And yes, there are advertisements and paper newspapers, but the newspaper is not looking back at you when you're looking at it. The paper one isn't. The electronic newspaper is.

And I think if you explain that to a consumer, which I why I think we have these sort of privacy panics every few months, people do get nervous. They do think there is a danger. They do think to use -- for lack of a better phrase, which is what the context is based on -- they do believe that the contextual integrity of their relationship has been violated.

So I think it's very, very dangerous for us to say, for the FTC to say context alone is all that we do. We have to think about what the context in the minds of the consumers are if we're going to go the context route. I think that context is very much tied to old analogies, phone companies, books, libraries, newspapers, rather than media that looks back and tracks and targets profiles.

MR. SOLTANI: I'm sorry. I do think there's

still some value there. I absolutely agree with Neil. But the model, instead of kind of books and newspapers, we might just put it around people. People we know and people we don't know. People we're engaging in and interacting with, and as Dan put it, everyone else.

I think the similarities between things like DPI and third-party advertising is that in the context of DPI and in the context of prolific third-party advertisement, there are people that are interacting -- that might be the Washington Post that are serving the ads or the New York Times or the Wall Street Journal that's serving the ads as they're meeting their content. But there are a handful of people that I don't know about who don't have a relationship that monitors my activity on the Washington Post or the New York Times. Maybe that's okay that they provide the ads, but those same people also monitor me on the other site, so I go to the New York Times. The same person that I don't know will monitor me on the Wall Street Journal and on whatever other sensitive site, WebMD that I go to, and they aggregate a link of that activity.

I think that aggregation across these different contexts of people that I don't know is what the sensitivity is. If it was each of the first parties, you know, if I engage with Facebook and Facebook knows quite

a lot about me, well, at least I'm aware of what they know about me. But if I engage in Google and they know a lot me from my search history, I'll be saying no to this type of information. We're not here to discuss it, but it's good to point out. It's the fact that even when I'm not engaging with Facebook and I'm engaging with the New York Times or the Washington Post, Facebook learns more about me or Google learn more about, but I think it is of concern and I think that's why this first-party/third-party discrepancy -- or description is helpful.

MR. ALTSCHUL: Well, it's important to keep in front of your mind that while we need to be aware of sensitive to the sensitivities, in terms of policies and prescriptions, we really remain focused on the heart. For almost anything we can imagine concerns and factors that we need to be sensitive to, but in terms of policy, we want to address and police the parts that we can identify.

MR. SOLTANI: I have a policy of not inviting my mom out on dates with me. Part of the reason is I don’t want her showing photos of me as a kid, especially if it's a person that I'm interested in.

MR. TIEN: You can’t stop it.

MR. SOLTANI: I can't stop it, but I can enforce certain policies that will likely provide that

outcome. That option doesn't exist to me to minimize the context collisions on the internet and I think that's a concern.

(crosstalk.)

MR. LINCICUM: On that lovely image, I think we have to move on because we are right at the time. I'm going to ask everyone's indulgence to let us go for just a few minutes because there are a couple of questions I want to hit and there are a couple of audience questions that have come in.

I will just ask the panel members to remember that we are a little tight for time, but I do want to ask you a couple more questions about looking forward a little bit.

The first question I'm going to ask you is, are companies really competing over privacy at this point? Are we seeing products that are offering more choices to consumers about how much of their information they share online?

Anyone can answer that.

MR. ALTSCHUL: I mentioned that I think that we are, in browsers, compare Chrome's practices to Firefox or for wireless text messages, the WhatsApp service to the Apple messaging or carrier text messaging. We are seeing differentiation of the marketplace based on

advertising and privacy practices.

MR. ERICKSON: Yeah. I think, you know, it's no doubt it happens in various ways. You know, the search base, there's a startup called Duck Duck Go, which promotes -- its product is not retaining any information about your search queries.

Sticking with the search query space, you know, a number of years ago there was a lot of debate about the retention of search query data and you saw sort of a war, almost, between a number of search engines around how long they were going to retain their search query data and they were competing in that space. We've seen that in the browser space and social networking space.

I think Google Plus has tried to advertise that product as something that gives you more granular choices than others. So no doubt it happens. There's a marketplace for that and I think companies make specific marketing decisions around and promote those privacy choices.

MR. TIEN: I wanted to throw in that we see this is the Do Not Track context. I mean, there are a number of companies, you know, Firefox was already mentioned and Microsoft is another one, where there have been some very, very significant initiatives to advance the privacy goal. But one of the enduring problems in

this area is because the technology is complex and because the consumers do not understand exactly what is going on, I fear that -- or I really believe that while they're trying to compete on privacy in some of these areas, the message doesn't get through very well because consumers don’t have as much of an appreciation of what the impacts of a particular feature might be or because sometimes the privacy concerns get out there in such a way that they are sort of indiscriminate. So it makes it harder for a company to stand out even when they're trying.

MR. SOLTANI: Yeah, just to add to that, it's hard to compete on something people don't know about. So if a lot of the collection is invisible or it's hard to differentiate, where we handle this invisible stuff better than the next guy. We have seen some companies make attempts to use it as marketing. Microsoft has done quite a job with Do Not Track as a marketing plan, but that's specifically Dean and the IE team really trying to leverage that as a product-positioning placement, but other parts of the organization would need to come along, like their ad-less ad network.

I think there are opportunities there, but, again, it needs to be comprehensive. WhatsApp is also known as the most insecure app. For a long time, for

about a year, it would allow anyone to access anyone else's full text history by just spoofing their phone number. That's quite easy and there have been a lot of write-ups. So I'm always reluctant to push one over the other because it's not comprehensive.

MR. RICHARDS: And then there's no better evidence that consumers don't know what's going on. In fact, we had a very interesting one-hour talk with Dan to start this daylong conference and the number of questions that we received about what is going on.

MR. BEALES: I mean, there a whole lot of markets that work extremely well even though consumers have no idea about how the underlying technology works. The computer itself, where that market works just fine.

MR. RICHARDS: But this is a market where the consumers are involved in a bargain over their data and the consumers don't understand what data collection is going on as the very basis of the bargain. And where that's happening, that is not the kind of marketing -- I don't need to know how an airplane flies in order to become a passenger on an airplane, but if I am selling -- if I'm buying a free service in exchange for a profile of my personal data, I need to know what's going on, what I'm selling, if it is in fact a sale or a transaction in order for that to be a fair and non-deceptive --

MR. BEALES: If you think about computers, where people have no idea what was going on for the vast majority of computers, but some people their games ran too slow and people pushed video chips that would accelerate the processing, designed specifically for games. There is a small number of people who know about that, you know, those that are interested in that attribute. That attribute spreads. Or think anti-lock brakes, consumers have no idea of how anti-lock brakes works. They're perfectly willing to buy the safety benefit. The problem in the market, when these things fail, if they fail, and we don't know that yet, but if they fail it's probably because there's not enough consumers who care.

MR. RICHARDS: With graphics cards -- and I was one of those consumers -- consumers can see -- I still am one of those consumers -- consumers can see that their 3D games are throwing out lots of triangles and that the frame rate is high. Consumers cannot see what is going on with their data because it is opaque and that is a fundamental difference. I think Howard is just inaccurate about the analogies of those kinds of markets.

MR. SOLTANI: I think a better analogy, and this might be a little inappropriate for this audience, but imagine if --

MR. LINCICUM: Go ahead then, Ashkan.

(Laughter.)

MR. SOLTANI: So I've decided I'm going to quit privacy and start a hotel chain. An international hotel chain that allows travelers to stay for free, right, and the only catch is that the travelers that come through my hotel, I have cameras installed. I blur out their faces and tattoos, but I sell it as a porn site to fund my hotel, right.

So for most consumers there's no harm. They're recorded, their data is being used, but they're getting this great service for free and they don’t even need to know about it because the hotel operates and they get a free service --

MR. ALTSCHUL: Isn't that the Chelsea Highline Hotel in New York? Doesn't it already exist? It's a little pricey.

(Laughter.)

MR. TIEN: So much for your startup.

MR. BEALES: That's pretty clearly a harm.

MR. ALTSCHUL: Why is that a harm?

MR. BEALES: It's been a harm at tort law for ages. You can't use somebody's image.

MR. SOLTANI: Even if I'm blocked out of the picture?

MR. BEALES: That's a harm. Reasonable people think that's a harm.

MR. SOLTANI: Why couldn’t you use my data which is very much my likeness?

MR. BEALES: Reasonable people don't think that's a harm.

(Laughter.)

MR. LINCICUM: That's a sufficiently loaded question.

MR. BEALES: Some reasonable people do. It's not a tort because --

MR. LINCICUM: Because the law has never seen that?

(Crosstalk.)

MR. SOLTANI: I'm trying to ask, what’s the problem?

MR. BEALES: Our privacy law isn't limited to tort law.

MR. RICHARDS: We have lots of them, and idea that privacy law is no different from what Warren Brandeis wrote in 1890 is just absurd.

Limiting things to tort-specific harm, you know, are we going to require physical injury in order to have privacy harm? I think the idea of --

MR. BEALES: That's pretty clearly --

MR. RICHARDS: I think it is one thing for us to look for problems, for dangers, for risks, but we don't usually look for harm -- we don't need to look for physical harm or sort of, you know, sort of front page news.

This is horrible thing has happened to this person because as somebody, I think Ashkan, said before, when we're talking about the aggregate benefits, we look at societal benefits from new trends and from traffic safety.

Why can't we look to societal benefits from privacy? Like, people able to read freely and not be deterred. We can't measure if someone doesn't read a certain kind of subversive or political article because they're afraid they're being watched. But if they don't -- if we're shaping our political discourse, if we're shaping our reading, that, in Howard's terminology, is a harm.

But I think that much more pointedly, it's a danger. It's a risk. It's something we should be concerned about. It is possibly an unfair practice or a deceptive practice. That's what we're here to talk to about. We're not here to write narrow, solely tort law focused notions of harm.

Privacy law is much more broad than that and

the consumer's interest in these kinds of technologies and these kinds of dangers, rather than harms, is much more broad than that.

MR. LINCICUM: All right. It's getting interesting and I hate to cut it off -- why couldn’t you get started fighting earlier?

(Laughter.)

MR. LINCICUM: I think we're going to have to start winding up a bit because we are officially over time at this point.

I want to ask one audience question, and I apologize to everyone whose questions we weren't able to get to. As you can see we had a lot of talk about. And then I'm going to ask each of you to give us kind of your sum up thoughts in very little time. So can start thinking about that now.

Let me ask you the question first. We had an audience member who asked -- and this is actually pretty relevant to what Howard was just saying. If things are changing, if things that are being collected are new, if they are creating new harms and new dangers, maybe we're looking at a paradigm shift. Are there ways that consumers can affect this individually and more broadly?

In other words, are there things that they can individually do to prep themselves and more broadly

affect the discussion and make their interest in this known?

MR. ALTSCHUL: Well, consumers do. As I said, the well-publicized sort of user rebellion against say, Facebook changes, in terms of service, reflect a very high level of sophistication among a very large number of users that do push back and affect the kind of privacy protections and policies that are provided.

MR. SOLTANI: Yeah. I think if they know about it, consumers will pushback about a lot of things that they know or made aware of, but as Howard pointed out, most people don’t know how their automobile functions and they don’t know that a lot of this ecosystem is powered by their data, just like I don't own my hotel.

(Laugher.)

MR. LINCICUM: All right. Let me go ahead and give you -- I originally said a whole minute, but we'll have to cut it down. You've got 30 seconds. You've got two sentences. Tell me what your sum up of your thoughts on this matter is. We'll start with Mike and just work our way down.

MR. ALTSCHUL: Well, to paraphrase the movie from a year or two years ago, it's complicated. There's no one single place or choke point that we need to pay attention to. We really need to focus on what it is that

policy and policymakers want to accomplish. What are the harms that need to be prevented or policed against?

And just as water seeks its own level, you try to squeeze or focus on any of the different layers in the stack, the conduct will find its way to another layer. So a bit of a Fool's Errand, looking at the layers to encourage everybody to look at the harms and the problems you want to address.

MR. RICHARDS: I would agree with all of that. I think we have to look at the dangers and also the values that are threatened by the collection data about all or most of your activities across multiple platforms.

I think we need to talk about, you know, we're creating a society where there's a massive market in all of our reading habits and all of our search queries, potentially. And I think we need to worry about that. We need to worry about not just intellectual privacy, but also about the power and balances for individual consumers, about limited consumer attention span when they are operating on multiple platforms at multiple times and also at the lurking threat that there is a potential for government access to these massive, highly detailed, highly sensitive databases.

MR. SOLTANI: I think we're going to look back on this and find how ridiculous that we were at this

point in time, the same way that we look at countries or companies being able to go into certain nature reserves and extract all of the resources with no recourse. I think there's an opportunity to demonstrate that there is a great deal of value in this information, but this information is co-owned between the people that generate it and the people that collect it and data mine it. I think, along these lines, there are opportunities to actually do better, in terms of providing high quality data the consumers knowingly and willingly engage in exchange for that information, and them leaving information that they find. So it's sort of I don't want to participate or sell in this marketplace off the table.

MR. BEALES: The Commission and the privacy regulation effort, in particular, should focus on information and its uses. It should do that in order to seek to avoid bad consequences for consumers. That doesn't mean, as I think I pretty clearly said, narrowly physical or economic harm. It includes a lot of reputation kinds of harms as well. But if you can't articulate what the harm is, you cannot prevent it.

If the only harm that we're worried about is speculative possibilities on what might happen at some point in the future, there's always going to be

speculative possibilities of what might happen at some point in the future. What we're likely to do is preclude a lot of really useful news services on the horizon that none of us have ever thought of yet.

MR. ERICKSON: You know, I agree with the statement that we should worry about the different implications in this debate and I think that's why this forum is good. There are other forums that WC III, Future of Privacy Forum -- people are doing a lot of thinking about this. The questions that we're asking today are the same questions that we've been asking for as long as people have been collecting information.

It's very, very hard to come up with comprehensive specific ex-anti rules. We've been trying to do that for a long time. So again, I think you have to default into what are the uses of data and the harms in order to prevent the collateral problems of overregulating and creating unintended consequences that involve the harm and the free flow of information. Thank you.

MR. TIEN: I agree with Ashkan and Neil, especially, but the thing -- the word that I want to emphasize is fairness or unfairness because they think that we are seeing two very, very different level at which there is a fairness problem. But first is simply

at the extraction and collection or sort of inducement of information about and from consumers, without any knowledge or understanding of who is collecting it, what is being collected and what it's being used for. At the other end of it, you have the fairness problem surrounding the uses.

I mean, there have been some great stories in the last couple of months about credit scores and e-scoring and all of the different ways that people are being judged and decisions are being made about that based upon this kind of information, and also based on algorithms for means the scoring for which the criteria are completely untransparent. So you have on the one hand, the input side of the data and on the other you have the judgment side about that and there are significant questions of fairness that are tied to privacy but are distinct from privacy for both of those processes.

MR. LINCICUM: All right. Thank you very much. I want to really thank the panel. They have been absolutely fantastic.

(Applause.)

MR. LINCICUM: So we're going to go to lunch now and we'll get back at 1:30. I hope everyone has a nice lunch.

(Whereupon at 12:17 p.m., a luncheon recess was taken.)

* * * * *

A F T E R N O O N S E S S I O N

- - - - - - - - - - -

(1:38 p.m.)

MR. LINCICUM: All right, everybody. Let's go ahead and start. Thanks for everyone coming back after lunch. Appreciate it. And now we're going to have remarks from Commissioner Maureen Ohlhausen. Thank you very much.

(Applause.)

REMARKS

COMMISSIONER OHLHAUSEN: I haven’t even said anything yet. I appreciate that. And thank you, David, for introducing me. And welcome, everyone, to the afternoon session. I heard the morning session went quite well and I look forward to, you know, continuing that good discussion this afternoon.

So to briefly recap this morning's session, Rice University professor, Dan Wallach provided an overview of the topics to be covered today -- this is awfully close to me -- including a description of the current technologies involved in comprehensive data collection.

He discussed current and possible future uses for this type of data and data profiles, and next, we heard from a panel of experts discussing the benefits and

risks of this type of collection. They indicated that comprehensive data collection incentivizes innovative new services and products and supports the model of the free internet. But conversely, they warned, the practice can also raise the risk to consumers' privacy in cases where the data is hacked or used for unintended purposes.

This afternoon, we'll switch gears a little bit. The first panel will examine consumer attitudes about and choice with respect to comprehensive data collection and it will focus on what data collectors need to do to inform consumers about their practices and to provide meaningful choice.

I hope the panel will also provide insights into what consumers already know and what they should be told about such data collection choices that are available to them about data collection and existence of competitive alternatives that offer different data collection practices to them.

And then the last panel today will offer a framework of how policymakers should think about data collection practices in an environment where companies are increasingly offering integrated products and services. What are the potential next steps for policymakers and industry and is the market working to protect consumers or does more need to be done, through

self-regulation or enforcement legislation or other regulation.

So obviously, as you all know, a major challenge for industry and for regulators in the area of privacy is the fantastic pace of technological change. It was only two years ago that Apple introduced the iPad tablet, which is really to believe that it was only two years ago. That device and others like it have seriously changed how consumers view and use their computers. And sales of tablets are expected to eclipse sales of PCs in the very near future.

Smart phones, the prevalence of Smart phones have also exploded. They have become more like PCs, by including internet access, browsers, maps, video music and all kinds of other services and increasingly, new forms of payment through mobile systems.

Many companies, such as Microsoft, have shifted their business model from exclusively selling software for all types of computers, to also marketing devices, such as tablets and things like Smart phone operating systems. And indeed, this integrated products and services model is now so much the norm that companies who don't engage in this risk are falling behind.

So our task today is to consider how these changes may impact comprehensive data collection and what

that means, both positively and negatively, for consumers. Yesterday, the Future of Privacy Forum released an interesting report entitled, "It's not how much data you have, but how you use it."

In it, the authors argue that their quest -- that in their quest for an integrated user experience, "Consumers are unlikely to object where the use of personal data is contextually consistent or where other circumstances weren't data use for an integrated user experience."

They observed that consumers want products that provide smooth operability between hardware operating systems and software, and that meeting this demand means that data provided for one purpose may be repurposed for another coordinated service.

So I believe that the greatest challenge facing policymakers in this arena is how to balance our consumer privacy concerns with the important goal of supporting innovative uses of technology and data so that consumers benefit from these advances without suffering harm from the misuse of their data.

So in the FTC's privacy report from March, Protecting Privacy in an Era of Rapid Change, the Commission emphasized the importance of context with respect to the need to providing consumers choice before

collecting data. The report stated that if data collection and use practices are consistent with the context of the transaction, consistent with the company's relationship with the consumer or as specifically required or authorized by law, offering consumers a choice wasn't necessary, but conversely, for practices that are inconsistent with the context of their interaction, companies should provide consumers with a choice.

Interestingly, when it issued the final report, the Commission changed from its earlier approach of listing five categories of commonly accepted data practices for which companies would not need to provide consumers with choice. And these categories were product fulfillment, internal operations, fraud prevention, legal compliance, and public purpose, and first-party marketing.

While I think that these are still appropriate categories, I believe the shift was more the result of the Commission recognizing that context can be quire nuanced and that we really need flexibility in evaluating consumer-specific -- I'm sorry -- context-specific consumer expectation. So over time, uses may change, consumer expectations may change, so we didn't want to be too locked in to, you know, specific types of uses.

The Future of Privacy Forum report suggests that the relationships that involve data collection will and should change over time. So it's not just the FTC's report that recognized that this will be a dynamic kind of relationship or a dynamic process, others have recognized it as well. And as companies expand their brands into previously untapped markets, the consumer relationship will expand to meet the consumer expectations.

So using the approach articulated in the FTC's privacy report, the context of a transaction or relationship shaped by consumer expectations will legitimize new data practices.

This approach that they suggest appears to make a great deal of sense to me, and provides the flexibility necessary to address the ongoing challenges created by this innovative and fluid industry. But of course, the FTC is not the only industry interested in privacy oversight. Over the past few years there have been a variety of proposals in Congress, dealing with privacy and data security.

Now, of course, last month's election substantially altered the congressional landscape on the privacy front. Several members who had key roles in the privacy debate, such as Representative Mary Bono-Mack and

Cliff Sterns, will not be in the 113th Congress. And as some of you may have heard, just today, Senator Jim DeMint announced that he will be leaving the senate to actually head up the Heritage Foundation. So there's going to be a whole change in the players in the congressional debate on this issue.

Other new members, such as Representative Lee Terry, will have leadership positions on the relevant committees with jurisdiction in this area. You know, in the last Congress, despite dozens of hearings and bills, we are approaching sine die adjournment without any significant legislative enactments in the area of consumer privacy. You might ask why, why did this happen.

There was a lot debate or a lot of discussions and hearing, but it's possible that this may reflect the fact that there really isn't a clear agreement on what the contours of what consumer harm may be occurring the market that current law can't reach, and what may be an effective and workable solution to addressing any harms that are occurring.

I look forward to working with my colleagues at the FTC and on the Hill in the next Congress to discuss to any legislation in the privacy arena in the future, but for now I wanted to offer a few basic principles

which I believe are important to keep in mind when considering any regulatory framework for consumer privacy.

I believe any privacy regulation should focus on whether particular types of data collection and use may harm consumers and violate their legitimate privacy interests. There should be a focus on providing consumers more tools, such as Web icons or opt-out mechanisms and ways to delineate and express their preferences, and market-based approaches, paired with self-regulatory initiatives should be allowed to continue to develop.

Government privacy regulation shouldn’t pick winners and losers based on technology or business models, particularly in a rapidly evolving and expansive internet marketplace. I believe a technology neutral approach that focuses on the impact on consumers preserves flexibility and helps promote innovation and competition among different types of entities.

And I believe that any framework should recognize that in today's dynamic internet ecosystem, consumer information can support legitimate and beneficial online services and applications. And as services evolve across multiple platforms, consumer data can be useful in generating new business models and

ultimately increasing consumer choice. So that's the kind of balance that we need to strike between consumer harm, consumer expectations and also some of the benefits that consumers may get from new and innovative uses of data.

Having said my piece, I'd like to introduce the first panel of the afternoon to talk about consumer attitudes about and choice with respect to comprehensive data collection.

So please welcome Alessandro Acquisti, professor from Carnegie Mellon University; Christopher Calabrese, legislative counsel at the American Civil Liberties Union; Lorrie Faith Cranor, a professor also at Carnegie Mellon University, and Michael Hintze, associate general counsel of Microsoft. So I thank you for having me and I look forward to the next panel.

(Applause.)

* * * * *

CONSUMER ATTITUDES ABOUT AND CHOICE WITH RESPECT TO COMPREHENSIVE DATA COLLECTION

MS. RACE-BRIN: Hi, everyone. Welcome our second panel of the today on consumer attitudes and choice with respect to comprehensive data collection. My name is Katie Race-Brin and I'm an attorney here at the FTC, in the Division of Privacy and Identity Protection. And I will be co-moderating today's panel with Paul Ohm, who is a law professor at the University of Colorado, and a renowned privacy expert. We're very happy to have him here doing a detail with our Office of Policy and Planning. So thank you, Paul for being here.

The purpose of this panel is to talk about choice mechanisms and consumer attitudes when it comes to the type of behavior we're been talking about today, a comprehensive data collection. We will discuss what consumers know about the kind of data collection that's taking place, both on the Web and through mobile devices. And we'll also address topics of transparency and consumer choice, including when transparency is important to consumers, what choice mechanisms are effective in this area and what are the limits of choice.

As a reminder, we will be accepting questions in various ways. For those of you who are here, you have

comment cards in your -- or question cards on your materials that you can fill out and hand to our FTC staff. For those that are viewing our webcast, you can submit questions through our Facebook page, through or Twitter feed, #ftcpriv, or by email at opa@ftc.gov.

I also wanted to mention that Professor Dan Wallach's presentation, for those of you that might have had problems seeing it before, is now available on our webpage. So you might need to refresh your browser but it should be there.

So I would like to introduce our panelists and thank them for participating today. We have Lorre Faith-Cranor, professor at Carnegie Mellon; Stu Ingis, counsel at DAA, the Digital Advertising Alliance. We have Alessandro Acquisti, professor at Carnegie Mellon; Christopher Calabrese, legislative counsel at the ACLU, and Mike Hintze, chief privacy counsel and assistant general counsel at Microsoft.

I would like to lead off with you, Lorrie. You've done a lot of research in the area of consumer attitudes about privacy. What does your research tell us about what consumers know and think about this type of comprehensive data collection that we've been talking about?

Do we have a sense of what really matter to

consumers when it comes to their information that is being collected?

MS. FAITH-CRANOR: Sure. So we've done a lot of research and other people have done research as well on consumer attitudes. I don't think there's been much research specifically on comprehensive data collection, certainly not couched in that particular term, but I think there is a lot of useful research about other types of tracking and data collection, which I think sheds light on this.

So when we've done interviews with consumers, we found that when we asked them about things like online behavioral advertising, most of them have very little understanding of it. They have very little understanding of most of the types of data collection that takes place, except for the data that they actually type into forms, you know, or they knowingly have collected.

So their first response is that this seems very creepy, very scary. They feel like it's happening behind their backs. On the other hand, if you explain it to them and explain why it's done, then they get kind of a mixed reaction. You definitely have people who see that there may be some value in this. I can see how I might be getting some customized services that I like. But on the other hand, they also feel like, you know, I seem to

have just given a blank check for these companies to collect all my data and do whatever they want with it.

They often have misconceptions about how it might be used. We had a lot of people we talked to about online behavioral advertising, who started talking to us about identity theft. So there are a lot of misunderstandings and are not really sure what is going to happen to their data.

We also find that some of the efforts that have been made to try to inform consumers about the data collection are things that haven't noticed. So we surveyed over 1,500 people and almost none of them recognized the Ad Choices icon. So this was not communicating to them anything useful.

We also found that when we asked consumers how they'd like to make decisions about this data and we showed them some of the tools available to them, a lot of these tools asked them to decide between different companies and they looked down the list of companies that do tracking, do behavioral advertising, and they didn't recognize the names of any of these companies. So they really didn't know how to make a decision about them.

Even the companies they did recognize, you know, Google, Microsoft, Yahoo, they didn't actually associate with advertising. So they were a little bit

confused as to why they were on the list and why they needed to make a decision about that.

We found that instead, users were very concerned about context. Users would tell us, well, when I'm booking my plane tickets, you know, some users would say, you know, I think it's great if some companies know that this is what I'm doing and then they can tell me about activities I might want to do at that location. And other users said, no, this is terrible because then people will know when I'm not going to be home and I'm really concerned about it. So different context, different users, had different opinions and it was really quite nuanced.

MS. RACE-BRIN: Great. Thank. Professor Wallach and our first panel discussed the various types of comprehensive data collection that may occur through ISPs, the operating systems, browsers, social plug-ins and the like.

Mike, you, at Microsoft, is a leader in the area of browsers and operating systems, both desktop and in the mobile context. What are consumers expectations concerning data collection for those various technologies?

MR. HINTZE: I mean, I think it's important to point out that there is a big gap -- at least in our case

and I think in many others -- between what a company could collect as an operating system manufacturer, browser manufacturer or in other context in what they do actually collect. I think a lot of what is driving that is consumer expectations.

Take some examples of our Windows product. Windows is the operating system, as was pointed out earlier today. The operating system is at the center of what you are doing on your computer. So, you know, it could have been a keylogger in Windows. There isn't.

Windows does collect some data, but it's very limited and it's done with a very deliberate decision around privacy in mind. One example I often use is the crash reporting. When Windows crashes -- you know, hopefully not very often -- you get a little dialogue saying, hey, information about what just happened on your computer can be really helpful to us to help improve the product. Will you send that to Microsoft? And you have to opt-in to that.

In some cases, there's actually a little bit more data about what you would be doing to be helpful and there's like a second opt-in in some cases. But the point is, it's an opt-in. It would be really useful for us if we got every crash report. But in the balance between what's useful and ultimately benefit all users of

Windows and what would be creepy and way beyond a user's expectations, that's where we came out.

We get enough data to accomplish that beneficial use of data that was talked about a lot earlier today. But we did that in a way that doesn't exceed user expectations. That's kind of how we think about it in all the things we do, whether it's the operating system or whether it's our ad network.

We try to strike that right balance between how do you get the data that's useful that can be beneficial to the users of our services but not cross that line beyond what users would reasonably expect.

MS. RACE-BRIN: Just a quick follow-up to that. How do you, at Microsoft, determine what consumer expectations are. Maybe I can throw it out to the panel and say for those companies that may not consider consumer expectations or limit their behaviors based on consumer expectations, what are the alternatives there?

MR. HINTZE: You know, there is a variety of means --

MR. OHM: Hey, Mike we've got a request to lean in a little bit for the webcast. Appreciate it. Thanks.

MR. HINTZE: There is a variety of means by which we can determine --

UNIDENTIFIED SPEAKER: Use another mic.

MR. HINTZE: Sorry. Is that better?

MR. CALABRESE: Usually it's mic that doesn't work.

MR. HINTZE: There's a variety of means by which we determine what consumer expectations are. We've done our own research. We look at other people's research for sure, like Lorrie's and others. There is some interesting research that came out of the Peer Research recently that talked about that people not only say they care about privacy, but that they were actually making choices based on that. The research -- I jotted this down -- showed that 56 percent of users decided not to complete an online purchase out of privacy concerns. And 30 percent of users have uninstalled an app from their Smart phone because of privacy concerns.

We've supplanted that with some of our own research. We recently did research in four major markets: The U.S., U.K., France, and Germany to gage user's attitudes about online tracking and whether or not they think it goes too far. Not surprisingly, an overwhelming number of users said yes, they do think it goes too far and that people need better, easier to use controls around that.

In addition to that, you know, we sort of -- we read the papers like everybody else and we kind of see

where consumers have objected to things. We try to learn from the mistakes, not only of ourselves but of others, and, you know, kind of get a gage. In many cases it's a little subjective. It’s kind of a gut feel. What's crossing that creepy line? Where are users going to reject a data use or a data collection that might be under consideration?

So it's sometimes more of an art than a science, but there are a lot of factors that go into those decisions.

MS. RACE-BRIN: Great. Does anyone want to comment on the second part of my question?

You know, if we're using kind of gut feel or, you know, an overall sense of what consumers expect, you know, as part of the determination about business practices, where does that leave us for other businesses that don’t consider that?

MR. INGIS: Thanks. And thanks for having me here. You know, I think when I think about the best way to evaluate what consumers want and consumer expectations, I immediately start with the free market. People spend their dollars every day on the products and services they want.

When I look and listen to the various studies, I find them interesting. I mean, it's interesting to

hear when you cordon off one segment and ask a question in a narrow sphere. And I think that's interesting to see how it influences things, but the companies we represent, the members of the Digital Advertising Alliance, the DMA and others, many of them, the innovators want to actually set consumer expectations. They want to innovate. They want to change things, change the world.

I was just thinking about on Cyber Monday -- Cyber Monday shopping eclipsed retail store shopping on Black Friday, I think, for the first time this year, which was a remarkable number. But if you had asked all the consumers 15 years ago, when you could buy something on the internet, where they expected to buy -- what the consumer expectation was on where they were going to buy their holiday presents, the answer was going to be, you know, they were going to go into the retail store at the mall or they were going to look at a catalog and they were going to buy their presents. But the companies that we represent didn’t say, okay, well, we better not design great products and services in offerings that would entice people to shop online and get comfort online because of that or even because, you know, studies at the time, similar panels had come and said, geez, 78 percent of the public is concerned about shopping online. They

didn’t say well, we better not design those products. They designed them and they're the ones we all live, love every day.

MR. OHM: So Stu, if I could ask a follow-up then --

MR. INGIS: Sure.

MR. OHM: We have two propositions on the table. Mike says that his company does ask consumers about privacy in addition to the kind of price signals that they're getting back. I don’t think you were saying that it’s a mistake for companies like Microsoft --

MR. INGIS: No, no.

MR. OHM: -- to ask those questions. And so I think you were saying that you value more -- I'm putting words in your mouth -- the price signals that you're getting back.

MR. INGIS: I think you want to evaluate a bunch of variable, but I think at the end of the day, and we see this, you know, if you talk about newspaper articles or particular business practices, the market reacts. When they see a business practice they don’t like, they stop buying it. They stop dealing with the companies. So if you look at some of the advent of some of the best data innovators, a lot of our members in the last number of years, the companies we spend all of our

time with all of us, you know, online, wherever we are, those companies are innovating. They're doing great things with data -- great and responsibly.

MR. CALABRESE: Can I just -- not to sort of pick out any particular company, but it doesn’t seem to me that there's a particular marketplace here to compete in this particular vector.

I agree with you that competition has driven a lot of wonderful things in this country. It's not clear to me that consumers are able or companies are able to compete because I don’t see an underlying legal framework that a) presents these issues in a way that consumers can make a meaningful choice and have a certainty that those choices will be honored. And I also don't think consumers are, in fact, aware of how much of these practices, and I think Lorrie's research shows that.

While I appreciate that market does a lot of things wonderfully well, we also know it only functions if the consumer has information and if there is an actual ability to compete on these particular things. I don’t think data collection practices are an area where consumers really can get fair competition or any kind of real competition.

MR. INGIS: Just to respond and then I know they'll want to move on, but I think there is some

validity to the fact that we've got to improve transparency in the dialogue with consumers, but I don't think we start with that as being the defining premise of how a marketplace and consumer should evolve.

So to the extent of transparency and choice, since you've both referenced Lorrie's study, I can just think of two data points, having sit and listened to Lorrie's studies before, the last time I was in a room and heard a study of Lorrie's, it was with respect to the advertising option icon.

Unanimously, they had looked all over the world, all over the wild -- I think it was a month after we launched the program -- and they found three icons out of 10 million sites or something. It was nonexistent. But I don’t hear those studies -- those studies aren’t repeated now to show that there are icons everywhere. That icon is being seen now more on the internet across the Web than any other symbol, period, globally. That's unbelievable.

Talked about the penetration of iPad in two year, this is less than that. And then the other number -- Lorrie, I think you gave a number that said, you know, you talk to 1,080 consumers and none of knew the ad choices icon.

I listened in on a presentation you all made

just a couple of weeks ago and the number was 30 percent of people actually recognize icons. And then that seemed to be a critique. We thought that was fantastic. Thirty percent in a year and a half, every brand in America, every new innovative startup company would love that level of penetration.

MR. OHM: Alessandro, I know you want to respond, but I wanted Lorrie, just because there was a direct question about her -- I think he was offering to fund your next research. Although I'm not sure that's what he was doing.

MR. INGIS: I'd actually -- since we're doing studies on the ad option icon, just a phone call about how the program works would be a start.

MS. FAITH-CRANOR: Well, we have had some phone calls with some of your colleagues, but I'd be happy to have them with you as well. We did not find 30 percent; it was a much lower percentage. It was somebody else who found 30 percent. I don't know where they found those 30 percent of people because we didn't find them.

MR. INGIS: Somebody did. You're agreeing, though, that somebody found 30 percent.

MS. FAITH-CRANOR: Yeah. And I had a lot of skepticism their study, based on ours. We also did do a follow-up on the icon study as well and we did report

that there was improvement. It was about 18 months later, there was considerable improvement, but still nowhere near 100 percent.

MR. INGIS: Oh, it's ubiquitous.

MS. FAITH-CRANOR: Facebook still doesn’t use the icon. You know, they refuse to use it and they are a pretty major that does behavioral advertising.

MR. INGIS: Facebook, as I understand the Facebook practice, and I don’t represent them, but our program actually doesn’t require an icon. It requires enhanced transparency and I believe Facebook actually does do that quite well, and they're a unique business model. But even they are trying to figure out how to give transparency. All the companies are always trying to do better. So to say, kind of, it's not out there, it's everywhere.

MR. CALABRESE: I mean, if we're having a free flowing debate, I'll throw something in here. I do feel, though, that putting the industry who wants to track you, in charge of opting out tracking, seems like putting the fox in the hen house, right. I mean, how can I, as a consumer, trust you to opt me out when your entire business model is based on tracking?

MR. INGIS: I don’t look at that way. I look at it about it's the universe of businesses that want to

deliver to you every day the free email services, the free content, the free offerings, the unprecedented ability to use content, communications tools you could never dream of before, everywhere, every single day of the world --

MR. CALABRESE: But by tracking you.

MR. INGIS: -- and the public loves it. The public loves it. By anonymously, responsibly collecting anonymous cookie data to deliver you the fact that you're interested in a car advertisement, you might be an enthusiast.

You make it sound like tracking like it's stalking and murder. This is people anonymously setting benign cookies on your computer to say geez, this guy appears to be shopping for cars and there's a new Honda on the market.

MR. OHM: Hang on. Let's make this a little less free flowing and a little more structured.

(Laughter.)

MR. INGIS: Come on.

MR. OHM: It'll be free flowing enough. Trust me. I know that we have a tenuous grasp on this, so let's pretend for a little while.

So I wanted to speak for a while -- what I propose is we kind of also set up the presentation of

your research, which we want we want to do. Is that okay if I kind of ask you a question or do you want to have a quick response to what's been said already?

MR. ACQUISTI: Well, I will give a quick response, although this was so much fun. I don’t know whether I want to bring you back to boring academia. There is a quick academic response, though.

MR. OHM: Give the quick response and then we'll tell where you are.

MR. ACQUISTI: So in economics, we tend to rely on the concept of DBL preferences. We don’t pay too much attention to what people say. We want to see how they really act, and that's why pricing is such a powerful signaling mechanism of what people really want. This works for most goods; however, it just so happens that privacy, as an economic good, is a very peculiar animal.

It shares the characteristics of what our economists call an intermediate good, a good that you value only as a step to something else, such as you enroll in a course and you pay for the course and certificate to get a job. And a final good, a good that you value in yourself, such as going out for dinner at a nice restaurant. Depending on which element or side we focus on, consumers may act very differently. As a final good, depending on subjective preferences, you may not

care for privacy and live your life as an open book or care a lot.

And the problem is that even if you say you don't care, you often -- or if you say you care, you're often in a position of informational symmetry to answer what is really happening to your data. As an intermediate good, privacy is a means of something -- to something else.

Privacy is a protection from potential costs down the road which may happen if your data is abused, identity theft, hiring discrimination, healthcare discrimination, price discrimination, service discrimination. It just so happens that these costs are not born immediately. When you share information, you get immediate benefit of the like, the discount, the gift. The cost is down the road. Sometimes it's not there, but if it arrives, sometimes it's weeks, months, or years. And this makes it very problematic to rely completely on so-called DBL preferences to assess what consumers want.

MR. OHM: Does anyone have a quick response before I give it back to Alessandro?

(No response.)

MR. OHM: Okay. I really enjoyed the first panel. I thought they did a wonderful job. There are

only two critiques I would lodge, which I like self-reflection. 1) I believe there are women who can speak about these topics and I think we should've done a better job at putting more on the panel.

2) There's that awkward moment where the guy gets up and says, "I have a PowerPoint to answer that question." So we're going to do one of those right now. It's not smooth.

Shifting a little bit from what consumers think, believe, what their attitudes are and how we measure that, Alessandro, your work is more about notice-controlled transparency. So we were hoping you could present some of the findings you found, and if you have a PowerPoint, yeah, yeah, please go ahead and --

MR. ACQUISTI: Maybe. I just so happen to have a -- let check.

MR. OHM: For the panelists, we printed out copies. They're in front of you if you want to follow along.

MR. ACQUISTI: Thanks so much for allowing me to use the slides. I'm not very good at expressing myself, so I need the help of visual aids. Also because most of the work we do is empirical, experimental. We try to do experiments, trying to understand what consumers do, what they want.

As a caveat, I will add that the particular experiments that I'm about to show are agnostic, in terms of what is the value of privacy or whether privacy should be protected or whether consumers should protect their privacy or not. We completely stay away from the question. It's a crucial, very important question, but we stay away from it.

We simply focus on whether consumers can, if they want to protect their privacy, can protect it under current approaches. And in particular, we focus, with these examples I'm going to show you, on the problem of control and transparency. Because we are focused on transparency, notice and consent, transparency and control is the means of allowing -- empower users to navigate the privacy (indiscernible), and we wanted to see whether they are more systemic universal challenges at the core of control and transparency regimes.

We often do experiments with multiple, diverse users. Of course, a limited satire, only show one example of each set of experiments. There are many more from where they come from.

The first one is the product of control. You may have heard stories about when there is legislation, imposing people to wear seatbelts, people start driving faster. So if you feel protected, you start taking more

risks. Or you feel empowered by something, you start becoming overconfident. We wanted to see whether this applies to privacy.

In other words, rather than what the convention of wisdom is that more control means more privacy, whether in fact more control leads to more exposure or sensitive information to more strangers. So we did several experiments. The one I'm showing you -- and in fact, it's a reduced version of what we really did -- is the following:

We asked subjects to answer sensitive and insensitive questions about themselves. An example of an insensitive question was, "Are you married? Yes or no? An example of a sensitive one was, "Have you ever used drugs, cocaine or crack?" Yes or no?

The one group of subjects -- these are randomized experiments. So we randomly assigned subjects with different conditions. They believe that this is a survey. They do not know that in reality it's an experiment.

One group of subjects was told hey, you answer are voluntary. You are not compelled to answer any of these questions; however, if you do answer, you are giving us permission to publish your answer in the research bulletin that we will do for the results for the

research.

The other group of subjects saw exactly the same questions, only that they also saw a little check box that they had to check to give us, explicitly, permission to publish the answer. So other words, we made them feel empowered. They had the same level of control as the subjects in the first group, only that now the control was made explicit.

Now, the paradox of control would suggest that because there is a small but nominal cost associated with checking the box, the subjects will not checkbox, but will simply answer the question or not, depending on their subjective preferences. But in fact, our paradox of control hypothesis would suggest the opposite. That's precisely because we put the checkbox, the subjects will track it and it will become more likely than to answer the questions. And this is exactly what happened.

So in blue, we have the percentage of answers -- - of questions answered by the subjects in the so-called explicit controlled condition, the first one I showed you. In red, the percentage of questions answered in the second explicit controlled condition.

In splitting the conditions to two groups, less sensitive or less intrusive questions on the right, on the slides, are more sensitive questions. So you can see

a strong response in that giving my explicit control works, particularly strongly for the more sensitive question. It can even double the propensity to answer the questions and allow the publication of the answers. In reality, there was no difference between the two groups, only in the second, the power was made explicit. So the story is that more control to lead to actual more disclosure sensitive information to more strangers.

How about transparency? We have been knowing for a while lots of research reveals that in the current approach to notification, but full privacy policy doesn't work that well. Privacy policies are long. They are not read. They are complex. So we are trying to bypass that issue with simpler notices, such as (indiscernible) but what if there is a fundamental, more systemic problems that we actually cannot even avoid through simplified notices.

What if there is transparency in the decision-making which happens after you have been provided a notice?

What in fact what we observing online is the trickery of privacy, like a magician which asks you to focus on the left hand so that you don’t see what is happening on the right hand.

Specifically, what we did was the following, we

did a number of experiments in which we provided simplified notices to our subjects. This particular was with students and we provided information about their answers to a survey about their behavior at school will be use. And we asked them, in some cases, very sensitive questions.

Now, one group of students was told your answers will be examined by a panel of students. Another group of subjects were told your answers will be examined by a panel of students and faculty. We expected that the subjects told that their answers would be also seen by faculty would be less likely to answer the more sensitive questions, such as, "Have you ever cheated in class?" Have you ever plagiarized work?" Which would make sense, right, because it inhibits disclosure.

After providing the notices, we started asking the questions. So when we do this, we do, in fact find what we expected, which is the subjects in blue, who were told that the answers will also seen by faculty, are less likely to answer the questions than the subjects in yellow, who were told that only students would see the answer. What I have on the Y axis is their response rates to the different questions.

Here is the key, let's say that now we insert a delay between the time we give the simple notice -- you

imagine it as an icon that tells you "faculty will read," or an icon which says "only students will read." And rather than immediately asking the questions, we wait. Why? Because online, between the time you read the notice or you've seen the icon and you actually have to decide whether to engage or not in a potentially private or sensitive action, there is some elapse of time.

So how long do you think we had to wait to nullify the inhibitory effect of giving the notice which tells the subject that faculty will read the answers? Ten minutes? Five minutes? One minute? How about 15 seconds.

So in 15 seconds is enough to nullify the effect of the notice. Or if we also ask a privacy relevant question, such as, "Would you like to join on a mailing list?" So in other words, we redirect the attention, and this already the effect of the notice. So I'm not making this summary of the results. I'm not making an argument about transparency and control. Transparency and control are important. I'm making an argument against transparency and control used alone, disjointed from what OECD and FIPPs, the privacy principles told us are the important things, such as proposed specification, limitation, openness, accountability. Without those additional principles, the

notice and control become so -- almost meaningless.

They become weak because we know from other research, that the full settings frames are so much more powerful in effecting how people behave. In fact, in the worse case, they become an example of what in social science and political science have now started being called a process of responsibilization, which is a terrible term for a terrible process which is pushing responsibility on other people for a problem that you have created. Thanks.

MR. OHM: Thank you.

(Applause.)

MR. OHM: So as a follow-up, and I want each of the four other panelists to respond. And Alessandro, if you have more to add to this, I'd love that as well.

Let's bring the focus back then to the comprehensive data collection. I think neither Alessandro nor Lorrie purported to do research on that topic. So I don’t want to put the cart before the horse when it comes to notice. Is notice even the proper question we should be asking?

The FTC, obviously in its privacy report and for a decade has put a lot of focus on notice and meaning choice. And to give teeth to this, I mean, let's talk about specific examples. So pick your favorite topic

we've talked about. It could be DPI. It could be the broad spread of OBA. It could be something speculative that doesn't happen, like an operating system or the browser. Is notice the answer? Should we turn to more and meaningful notice as the way to kind of remedy the privacy risks versus the benefits that we see?

Lorrie, you first.

MS. FAITH-CRANOR: Well, I think notice by itself is clearly not the answer, but I think notice can be part of an answer. But I think at the very minimum, the notice has to go hand-in-hand with a really meaningful choice. And I think there also needs to be, you know, a backstop so that you can’t do things that are really unconscionable and say, oh, but I gave you notice. You didn't read it?

So I think that that is important. I think, you know, in addition to the research that Alessandro mentioned, we've also done research that's shown that the timing of the notice is critical. That you can show a notice at some points in the process and people act on it and at other points where nobody is paying attention.

Clearly, also, the format and how well you communicate with the notice. And then also, I think a big problem in comprehensive data collection is that the data collection is happening all over the place and all

the time. And I don't think we want notices all over the place and all the time. So if notice is going to be part of the solution, we need to find a way of giving notice that is timely and relevant but not all the time, or we're all just going to ignore it.

MR. OHM: And Stu, you've already instilled the virtues of the icon program. I mean, it seems like you guys have decided that notice isn't important.

MR. INGIS: A couple of years ago we were told we needed transparency all the time and so we've delivered that in a ubiquitous way. And yes, we're learning as we go. So I don't claim that that's the solution to all problems, but I think we're seeing, actually, good results.

We're seeing, you know, trillions of icons served and we've got, you know, I think it's almost 2 million opt-outs; 20 million people -- don't hold me exactly to these numbers -- but 20 unique users have actually gone to the choice page and most of them actually spend time there and decide not to exercise the choice.

Maybe it's actually along your theory, which is they see a reputable program and say geez, I'm okay. This is good. These are reputable brands that clearly a lot of responsibility goes into the program.

You know, as far as -- to answer the question is transparency enough, I think when we did the DAA standard -- and of course, it's always evolving with that recognition -- I think we actually did draw a line for comprehensive data collection which was a different standard than what we had had for traditional kind of ad network standard, but we were technologically neutral, right.

So whether you were a traditional ISP or you were a browser or you were a plug-in, if you were getting that level of comprehensive data, we held things to a higher standard.

I think what you really want is a notice that people see so they can get to whatever choice it is that is offered. In our standards, we had agreed that, geez, we need to pull privacy outside of a notice. We need to pull that transparency outside of a notice. So we did that in the form of the icon for kind of ad networks and those displays and where you see it everywhere.

With traditional ISPs or even plug-ins and otherwise, there wasn't the same ability, technologically, to do that. So had a scenario where instead of going to get that uniformed choice that's now available, there was no transparency to show how you could even get there.

So the standard that we coalesced around, from all parties, was a little bit of a heightened standard from enhanced notice, which is a consent, but it wasn't an expressed, affirmative, or opt-in consent, but it was a defined terms, which was a flavor higher. Whether that's ultimately where the world should go, you know, over time, we don't know. I mean, we're seeing all kinds of great concepts discussed where people that traditionally provide different services really can add lots of value to enrich all of our lives in a responsible way.

MR. OHM: So Chris, I think a lot of Stu's answers circulated around the follow-up I was going to ask you, which is, you know, does it really depend on the type of ISP -- sorry -- provider that we're talking about at a given time?

All day long, I think every speaker that has spoken has said we should be tech neutral. It should not be about the technology at all.

I mean, what's your take on different forms of comprehensive data collection and the need for transparency and notice, the possibility for transparency and notice, depending on the type?

MR. CALABRESE: Well, I also believe in tech neutrality, if for no other reason than the technology

changes so fast.

I have to say, I think transparency or the lack thereof, and I will say, I think it's failed up to this point, and not through lack of trying by a lot of people over a long period of time, but I don't think transparency in and of itself has worked very well.

I will offer a theory as to why that is that will probably be disputed by others on this panel. And that is people will not learn about things, will not actually sort of engage in a process of trying to learn about things and get more transparency unless there are other rights that they can exercise as a result and unless it's meaningful.

What I mean by that is, I am not going to bother to learn about a system if it's a take it or leave it choice. I am not going to bother to learn about a system if I realize, well, this is a system run by the people who are actually doing the tracking, so I don't trust this system. So I'm not going to bother to do this because it's very cumbersome.

Again, I know that's, you know, a position that's not shared by everybody, but I believe that until we provide an additional meaningful parcel of rights, and I believe that has to come legislatively. I don't believe that self-regulation can do that. I think that

those rights need to be imposed by legislation. Once that happens, consumers can actually learn about their choices and make meaningful choices and then I think transparency will have a very important role to play in how those rights are exercised.

MR. OHM: So Mike, I want you to follow-up, and I'll get others to follow-up on any of these too. On everything that was just said about transparency and notice, I have one little additional thing, which is change. A company like Microsoft will have practices on Day 1, different practices a year later.

What do you feel about, particularly comprehensive data collection, how does that affect your choices at the time of change when you decide you want to embrace more collection than you have in the past?

I mean, is there heightened notice or their heightened obligations? More due diligence on your part? What happens with that?

MR. HINTZE: Yeah. I mean, I think there are, but I would preface that by saying and echoing what I think other people have said is that transparency choice is 1) very difficult to do effectively. People criticize the icons because they're ubiquitous and therefore, everybody sees them and you ignore them.

People criticize privacy statements because

they're too long and nobody can spend that amount of time to read all the privacy statements that they encounter.

There are lots of ways to provide transparency. I think transparency is critical. I actually will defend both of those approaches and others. I think you need to approach transparency in multiple ways. I think the long privacy statements are important. When I ask people who say they should be short and simplified, I ask well, which facts that I'm currently telling consumers would you like me not to tell them? And people can't point to anything.

Even though consumers don't read them, folks like the ACLU do, journalists do, academics do, and it provides some level of accountability for the watchdogs to have that full complete information out there. The FTC does. I can attest to that.

(Laughter.)

MR. HINTZE: You know, you asked about change, when practices change. First of all, not all changes are bad, right. I mean, we've talk about in this era of big data that some of the really beneficially uses of data you didn't anticipate when that data was collected. You can do some really interesting things that are a public benefit, that are benefits, economically, that are benefits to end users. So change is inevitable. It's

part and parcel with innovation, which I think we all want to encourage.

If you have collected data under a promise that we will not do X with data and then suddenly you decide to do X, in my view, you need to get opt-in consent for that. If you want to change the program going forward and say from this day forward, this product is going to work this way and X is now part of it, I think you need to give a very prominent notice to current users so that they are aware of that. You can't trick people. I mean, that's the classic Section V deception if you go about it the other way.

MS. RACE-BRIN: You know, building off Mike's comments and some of the other panelist's comments about how notice is tough in this area, are there other principles that can help facilitate transparency, such as consumer access to data?

Is there a means by which consumers should be able to see the information that is being collected about them?

MR. OHM: And we're, of course, talking about other Fair Information Practices. I mean, are there other things on that particular menu that might fill in some of the void? Stu?

MR. INGIS: I think there is. I called them

actually prohibitions. I think they're the type of things Alessandro was referring to as the harm down the road. I think -- actually, back to your study, I think that icons and other symbols that give people confidence that are designed to give people confidence for responsible practices are reinforced, be it through law or otherwise.

If you really, you know, identify the harms down the road we're talking about, in the DAA context, we said, you know, just the flat out probation, not even with the consent, you can't use data, this click stream data for healthcare treatment, for insurance, for financial decision-making, for employment. There probably are others that should be added and we'll probably, over time, will add to that list, but I think that if you really take off some of those harms down the road, we're all in a better place.

MR. CALABRESE: If I can echo that because, of course, that's 100 percent true and I think any time that we can take -- we can give consumers another mechanism to deal with harms they've suffered, we're in a better place as a society.

I think these are very hard harms, however, to put your finger on sometimes. It's difficult to know whether you've gotten a different insurance rate than

someone else, for example. To say that we can deal with the harms, perfectly, I think ignores the fact that the FTC, certainly -- I mean, maybe you do have the staff to deal with all those possible harms, but I suspect not. So there has to other intermediate rights that accrues.

I mean, one that I like is the Do Not Track mechanism. Something that is robust enough that, as a civil libertarian, as someone who cares about the First Amendment, I can hit a button and know that I can research a sensitive topic or I can research radical Islam without worrying that that's going put me on a terrorist watch list.

MR. INGIS: But, for course, legislating that may actually eliminate -- it may not be allowed by the first -- that very First Amendment you're trying to protect.

MR. CALABRESE: Well, I don’t think so, but it will probably take us off the track.

MS. RACE-BRIN: Alessandro and then Lorrie.

MR. ACQUISTI: Just to extent on what Stuart and Chris were mentioning, one of the OECD principles was accountability. We have had this problem or situation, depending on which side of the debate you are in, where companies which have violated either their own privacy policies or regulation.

In absence of actual provable harm have actually now been considered liable. So we are relying on a model where you have to prove actual cost, but to me, where the problem of privacy is going is that it's less about a cost and more about a transfer of surplus from the data subject or the data holder.

So it’s not identity or mainly identity theft because we will get better and better, maybe, in protecting ourselves from identity theft. It's more about, for instance, price discrimination, so that you are paying for a good .05 cents more than the next person. And as Chris was mentioning, you do not even know.

I feel that currently we are incapable to consider these, what I would consider privacy harm because unless there is some provable damage, there is no or very rarely there is a cause for action.

MR. OHM: So if I could just push you back on that a little bit because I'm sure -- and this isn't my usual mode -- but I'm sure there are economists in the audience saying, wait, wait, are you saying that all price discrimination equals harm or equals privacy harm?

Because on the earlier panel there was a conversation about price discrimination, but it's the good kind of discrimination, not the bad kind of

discrimination.

MR. INGIS: What about --

MR. OHM: I want to hear Alessandro elaborate a little bit more on that last point.

MR. ACQUISTI: So there are three degrees of price discrimination, first, second, and third. The funny thing is that when we start having these debates on price discrimination, one side of the argument is talking about the second and the third degree. And the other side of the argument is talking about the first degree.

The first degree is when each consumer has a certain type, preferences, a means to pay for a good. And in the extreme case, preferred price discrimination, is charged a price exactly at the level of the original price. That is probably efficient, only that all the surplus from that section goes from the data subject to the data holder. To me, that is problematic.

The argument that instead, an economist could make in defense of price discrimination is offering for second and third degree. When you say well, we allow people to pay very little for an economy seat on a flight because we are making the professionals who go business pay very much. And therefore, in a way, the professionals are subsidizing the low price for the coach seat. But there are two different types of price

discrimination.

What is happening with tracking is that we will see more and more first degree price discrimination because second degree and third degree can already be done either for self-selection, self-degree, or through showing a membership in a certain group, elderly, young, military or whatever else, which can be done without identification on the subject. But tracking is about first degree discrimination.

MR. OHM: Lorrie, did you have a follow-up?

MS. FAITH-CRANOR: Yeah. A follow-up on a few points that have been made. So I actually agree with Stuart on something. Amazing, right? On the need to have limitations of certain types of uses. And I think it's great that the industry guidelines say hey, there are certain things that you're just not allowed to do with the data. I think that's really good.

I'm still concerned that it's still just a guideline and there may be some companies that are not doing what the industry tells them that they should be doing. And a lot of these guidelines have not been very well enforced, and in many cases, not enforced at all, legally. And it would be nice to have some legal weight behind these things and not just rely on self-regulatory guidelines.

I also wanted to pick up on what Christ mentioned about Do Not Track another sort of alternative to a notice. You know, instead of making consumers look at notices all the time, just set up your browser with your preferences and let it act automatically. I think that's a nice idea.

There's a whole conversation about Do Not Track. I don't want to get into it right now. I think one particular aspect of it is that it was very simple. I think in the future, this comprehensive data collection is not going to take place just with users sitting in front of a computer. It's going to be taking place as we walk around the world everywhere. And it's not necessarily that you're going to own like, one computer and one browser and you can press the button and it may those billboards that you pass, you know, your shopping cart and all these devices you interact with are all going to be tracking you in all sorts of places and all sorts of different data. I think --

MR. INGIS: Sounds awesome.

(Laughter.)

MS. FAITH-CRANOR: I think we need to think in terms of how users can basically have agents that, perhaps, represent them in the world and can deal with all of these notices that they're going to be bombarded

with all time and all the decisions that they have to make and think about how some of these decisions can be made automatically.

MS. RACE-BRIN: Did you want to make one more comment, Mike?

MR. HINTZE: Yeah. I just wanted to respond to the initial question about whether or not we need a broader range of Fair Information Practices, and I think many people have already said yes. I just wanted to add my voice to that.

I think that in the scenarios that Lorrie has mentioned, where there is more and more ubiquitous tracking or data collection through more and more vehicles, whether it's, you know, toll bridge sensors or various types of data collection in shopping malls and online and offline and mobile and all of that.

I think we're going to get to the point where -- I think we're probably at the point where you can't have a notice for every one of those. I'm not going to stop my car on the bridge and read the notice above the sensor.

So we need to think about a broader range of Fair Information Practices, including, you know, the traditional ones that go back years and years. Collection limitation; you shouldn’t collect more data

than you reasonably need to accomplish the purpose for what you're collecting it.

Data retention limitations, you know, thinking about ways to minimize the privacy impact from the beginning through identification and anonymization, as Paul and others have written about, that's not a perfect solution either, but you need to think about all of these things as part of the toolkit, right. And you need to think about use.

I mean, we're not going to stop data collection in this day and age. It’s going to happen and there's going to be more and more of it going forward, but we need to think about limitations on use. And I think context is part of that, as many people have said. Some uses are just so obnoxious that we should prohibit them. And then there are a few uses were notice and consent will continue to play a role.

MS. RACE-BRIN: Thanks. I want to move into a more focused discussion on choice and context, as you mentioned, Mike.

In our privacy report, as been discussed numerous times today, we, the FTC, included a discussion that companies don't need to provide choice before collecting and using consumer data for practices that are consistent with the context of the transaction or the

company's relationship with the consumer.

So this becomes particularly complicated in the area of comprehensive data collection because, you know, as Commissioner Brill talked about earlier today in her opening remarks that a lot of this collection is happening in the background, running behind the scenes. So there might not be a one-on-one relationship with the consumer.

I'd like the panel to talk a little bit about how the principle, as outlined in our report, applies to the comprehensive data collection model or does it?

MR. INGIS: I'll take a first shot at it. My sense, I think that that principle -- I know people may have a different view of it -- but I think that's really a use principle in a permitted use principle on the other end of the spectrum from the prohibition that I talked about. As I think we're laying out choice -- and I don’t want to digress into the Do Not Track either -- but I think there is simplicity of choice where you can have one button that captures a whole product of services. I think the proponents of that type of solution in Do Not Track favor that. And there's also much more granular choices.

You can look at some of the settings by the Blue Guys or Google or others, where you can choose, you

know, what the inference is about you. You're an auto enthusiast. You're a car entendran. And they kind of have some of the flexibility. In the DAA program, for many years -- and FTC staff has worked on it -- always said, you know, do it one at a time.

Ultimately, I think there was a recognition; it was really the same exact practice. Not driving through a tollbooth, but the same practice companies many people hadn’t heard of, so we should allow both. You could pick a company at a time. If you saw a brand name on there you liked and you were okay with it, you could uncheck it. But there is one button where a consumer can go now. You can go now, actually, Chris, when you do your first (indiscernible) research, with one button and it works today, for anyone who has that concern and it's working for in the millions of people.

So to me, you have permitted uses. You have prohibited, and then in between, you have to have flavors.

MR. OHM: I'd love to ask a follow-up because you started the answer, making it sound like you were saying the one-stop shop nature of Do Not Track is not sufficient. And then you ended it, touting the benefits of the one-stop shopping in the opt-out section. Is there's a difference in degree?

MR. INGIS: Yeah. No, no. Right. Let me clarify a little bit. I think it is sufficient, one-stop shop. I think you have to have flavors, but it's one stop shop in what sector, right.

So I don't think one-stop shop for, you know, click stream data should also apply to whether you get a catalog at home or whether the toll booth is checking your meter. I mean, those are different things. So I don't think we're benefitting society by just saying let's have the paranoia button, the one button, you know -- that's not moving things forward.

So I think we have to figure out where are the areas, where are things so similar that it makes sense and where are the areas that are different that you need different flavors.

MR. OHM: Let me get other people involved with the consistent with the context conversation. All right. That's my FTC head; here's my other hat.

The privacy report, which I actually think is a masterful job, puts a lot of weight on this question of consistent with the context. And frankly, my initial inclination is that it makes me extremely nervous because everyone thinks it a great idea. So anytime everyone thinks it's a great idea, I begin to suspect that they all think it means different things.

So the question is, what does consistent with the context, when it comes to comprehensive collection, mean to you?

And if I can be a little bit more provocative about it, is consistent with the context advertising-supporting, internet service provision? Is that consistent with the context?

Well, of course we're going to turn DPI on because that's how we're going to give you a break on your monthly cable bill. Is that consistent with the context of cable provision? Or how do we decide?

Give us advice. Now that we've said that it's an important phrase, give us advice on how we interpret that important phrase.

And I'm a law professor, so I'm not afraid to call on you.

MR. INGIS: I'll just jump in again, quickly, which is I don't actually agree with consistent with the context. I think your first question was there are certain permitted uses, and so I agree with that. I think it depends. I mean, I think there are sometimes where we derive immense societal value on figuring data patterns out that had nothing do to with why the data was collected that's useful. And if we're going to restrict that, I think we're going to restrict some of the magic

in the world that we're figuring out right now.

MR. OHM: So we should just ignore context sometimes if --

MR. INGIS: Well, I think sometimes it works, but sometimes it doesn't. You know, I don't think it's just as clean as a bright line.

MR. OHM: Lorrie?

MS. FAITH-CRANOR: I think consistent with the context is very broad and probably too broad. I think that the original list of five points was much, much more narrow. There's a notion of kind of absolutely required for the transaction that I'm doing, which still can be misinterpreted or interpreted in multiple ways, but I think the notion that when I buy a product online, clearly you need my information so you can bill and so you can deliver it to my house. I think there would be a pretty good consensus that those are essential to the transaction.

Then you say, okay, well, what about sending me a catalog so that I would want to buy more things. I could see a marketer saying, well, you know, you're our customer and you like our product, so part of the transaction is sending you catalogs. I could see a consumer saying, no, you know, this is a one-time thing. The catalog wasn't part of the deal. So that's not part

of the transaction.

MR. INGIS: What if it's everybody -- we've noticed a lot of people buying Dimetapp or some flu medication and we've discerned that when that's happening, people actually buy a lot more orange juice and we're running out of orange juice in grocery stores. Should we be able to use that data to deliver orange juice so people can get orange juice?

MS. FAITH-CRANOR: I think that's a good question and I don’t think that the FTC's definition allows us to answer that question.

MR. INGIS: Right.

MS. FAITH-CRANOR: So I think what the guidance that the FTC is given is way too vague for anybody to do anything with.

MR. HINTZE: I don’t think it's way too vague to do anything with it. I think it's too vague to be the sole answer to difficult privacy questions.

MR. OHM: Well, it's certainly not. There are lots of other answers in the privacy report.

MR. HINTZE: Right. When I am going back to the office and getting multiple questions a day about should we do this or should we do that, that context in consumer expectations is certainly a very big factor that goes into those decisions. It's not the only factor,

though.

When I think about that concept, I think about it quite broadly. I think about it in terms of different degrees. We certainly don't want to do anything that when people learn about it they're going to be freaked out or surprised in a negative way.

I don't think the orange juice example would freak people out or surprise them in a negative way. I think that's probably a good use and that kind of use can be done, by the way, with de-identified data. You don't need to know that bought Dimetapp, and therefore, I'm going to by orange juice. You just need to know a lot of people bought Dimetapp.

So when you're making product design decisions, when you're making decisions any activity that is going to impact privacy, you need to take into account the context. You need to take into account what consumer reaction is going to be to it. And there are many, many, things you can do to impact that, you know, whether it's done in an identifiable or de-identified way. Whether it's done using, you know, whether you have given people a choice in some cases. What kind of notice have you given people?

There are just so many things that go into it that it's hard to sort of boil it down to a formula.

MR. CALABRESE: If I could, sometimes I feel like the debate in this area of big data generally turns to more of a boy, this data is really cool and we can do a lot with it. And the "we" is not generally the consumer. It's generally someone who's aiming and wanting to do something to the consumer.

The example that I think of here, and I think this comes from a New York Times story, where if Target learns a lot about you and they can target you directly and they know your income level, for example, they can learn whether I, Chris Calabrese, can be enticed into a target with a one dollar coupon or a ten dollar coupon because they know how much money I make.

If I was given the one-dollar coupon, I would never have the chance for the ten-dollar coupon, right, because they know that they don't need to give that to me. Now, that, to me, is a form of price discrimination. I believe it's enormously problematic because I do think it really harms the consumers, especially if you make less money.

MR. INGIS: What if the person making less money got the ten-dollar coupon?

MR. CALABRESE: But they don't because --

MR. INGIS: They do, actually. They do.

MR. CALABRESE: -- they have the data

collection --

MR. INGIS: Actually, they do.

MR. CALABRESE: If you're telling me that Target is going to give an extra nine dollars.

MR. INGIS: I'm not talking about Target, just general -- let's get off of that.

MR. CALABRESE: I shouldn't pick on you, but why? I mean, if I know that you make $20,000 a year and you'll come shop with --

MR. INGIS: Because in many cases, they want to move volume and they know that people -- you may not reach a price point that someone would buy. It's the same reason you have sales. It’s the same prices get lowered, generally. Our economist to speak to this, right. I mean, why is that certain cell phones are sold are lower prices -- it's because -- you know, they're started at high price? It's because more people can come in and buy them.

MR. CALABRESE: I'd be happy to -- if I could finish one thought --

MR. INGIS: Sure. Sure.

MR. CALABRESE: -- which is I do believe that we are -- when you collect an information, you don’t own it. The consumer still owns the information, without attaching property, legalistic concerns to it and you are

a shepherd of that information. You should use it in the minimum amount possible. You should anonymize it as much as possible. You should keep it as little as possible and you should essentially be serving the consumer when you are owning your data.

So the extent decisions are made that don't do that, I believe they are wrong. I think an information asymmetry does not serve the consumer. I think it serves the seller.

MR. INGIS: On that notion of you should serve the consumer, I agree. And I also think your broader point is yeah, data could be misused.

MR. CALABRESE: Is.

MR. INGIS: Your example, I think people probably come out in different places on it and I think part of the challenge is just figuring out what's a misuse and what's a benefit. It's complex.

MR. CALABRESE: Probably should let the consumer figure it out.

MS. RACE-BRIN: I think Alessandro has been waiting to comment. Alessandro. And then I have a question from the audience I'd like to ask.

MR. ACQUISTI: Two comments. One is about the price discrimination again. To me, it seems that the trend is clear and perhaps, inevitable. Tracking will be

used more and more, not just for advertising, but they need it for price discrimination. And the type of price discrimination that we will see increasingly out in the marketplace will be first, the reservation price discrimination, which means each consumer has a certain reservation price for a specific good and will become better and better at pinpointing exactly that reservation price.

The second point is more about, Paul, what you were mentioning in terms of when you hear everyone agreeing on the term of being concern. You made me think about the Rudyard Kipling poem, "If-." There is this beautiful line, "If you can keep your head when all about you are losing theirs...you are a man, my son."

I don't know whether you've ever seen the Murphy's Law version of that line, which is, "If you can keep your head when all about you are losing theirs, it means you didn't get the problem."

(Laughter.)

MR. ACQUISTI: So it's the Murphy's Law of privacy that if we believe that one term, one concept can solve all the complex privacy problems, maybe we didn't get the problem.

MS. RACE-BRIN: Great. Thanks. I'm going to move onto a question from the audience, talking about the

first versus third-party distinction that we talked about some in our privacy report and has been talked about quite a bit in the literature.

Does that hold up when applied to large, diversified entities, such as Google, with its ad network, search T.V., et cetera?

Do consumers really understand this and how does that affect their understanding of their relationship with the entity?

MS. FAITH-CRANOR: Yeah. I think consumers are fairly confused about this point. One of the things that we found in our interviews with consumers is when we talked them about who was tracking them and how, they said well, when I got to Google and I'm on their search engine site and I search for something, I understand that the ads that I'm going to see are directly related to my search. I understand that.

I also understand that when I got to Facebook and I tell them my age and my gender and where I live that the ads I'm going to see are going to be related to that. And then when we would say well, what about on other sites? How do you think you get Google ads or Facebook ads, or whatever, on other sites? And they had no idea. And they had no concept that the activity that they did on one site was going to follow them around to

other sites, and they weren't associating Google acting as a third-party on these other sites.

MR. INGIS: I think many consumers do understand it, bit to the extent some don't I don't think it's necessarily the right question. I mean it's a part of the question. The question is do consumers benefit from that sharing of data. In my life and what I do as a consumer, categorically, yes. Tremendous benefit. That's why there's this continued offering of services. And then, even within one company, you know, if you look at the DAA standard, for example, to the extent different companies are acting in different capacities, either as a service provider or an ad network, if they combined them, they wind up being treated to the more restrictive standard.

So there's not all this, you know, geez, it's just benefitting the companies if you combine data in different context. There are further restrictions, lots of policies that bind them.

MR. ACQUISTI: May I follow-up to that? I'm not going to argue that what you said is incorrect. I'm going to argue that we cannot really know whether this statement is correct or incorrect. What I mean is the following:

Behavior advertising is, in economic terms,

essentially a reduction of a transaction cost. Rather than spending 30 minutes looking for a product, you have this product appearing to you, which magically happens to meet exactly the criteria of something you were looking for, or at least this is what we believe.

The counterpart is that we don't know whether the customer, how long he would've spent or she would've spent to finding a similar product or perhaps, an even better product, or perhaps, a better and cheaper product. We don’t have the counter factor, and therefore, we cannot really conclude, right now, how good, for consumers, behavior targeting is.

MR. INGIS: But we do know for a fact, and economic studies show that if consumers aren’t aware of a product when they're making their choices that they're not well served.

So often, when there's behavioral advertising done, you're telling people about a product or service that they want at the time that they're interested in that they may never have heard about before. And the advent of this technology has solved that problem, economically, in more ways than --

MR. ACQUISTI: Maybe my point wasn’t clear. What we have in advertising that is a reduction is transaction cost. Transaction -- I apologize -- search

cost. You spend less time searching. On the other side, there is the issue of would the consumer, maybe you spent five minutes more, maybe one hour more, which is a cost, but found something which even better fit the consumer need. Maybe even a lower price.

This is a very difficult question to treat economically. It's incredibly difficult. No serious economist that I know of would dare try to quantify that because it’s exceedingly complicated, but I think it's a crucial question.

MR. OHM: Could you list the unserious economists?

(Laughter.)

MR. OHM: But I mean, I think the other part of that question is -- the suggestion seems to be on the table that were it not for behavioral advertising, the entire internet would become like a wasteland, right? We would all be roaming around with our mice with drool coming down. I mean, so the questions is -- the question is --

MR. INGIS: No. We don't know.

MR. OHM: Right. I think Alessandro's point is we don't know. And I know a lot of people cite a couple of studies, but here's my public call to all the economists out there. Study this more, especially those

of you at the companies who have the data, like, share it with us or study it yourself and release the study results. And Alessandro, I'm sure, again, will take funding to do -- I don't know why I'm playing matchmaker with the grant.

Anyone else on this point?

MS. RACE-BRIN: I wanted to just take another question from the audience that we were talking about choice and whether or not there is consumer harm when it comes to lack of choice. And this question is about the DAA's principles.

It says, if as under the DAA's principles, an entity collecting all or almost all consumer data must get meaningful consent to this collection, what is the harm or objection?

MR. OHM: You don't mean the harm to the collection, the harm to the consent.

MS. RACE-BRIN: The consent. Yes.

MR. OHM: Answer either one.

MR. INGIS: I'm not sure there is a harm, actually, at all. In fact, I'm not aware of any practices that would cause a harm. I think the way we approached it and kind of coming up with that is we were trying to provide a way to ensure transparency. People in that functionality didn't have a direct relationship

in that context, with either the consumer in that context. They do it in other contexts in providing the underlying service, for example. Or they didn't have a direct relationship or were not privy in any way, even indirectly, but in privity with the publisher. So we were just trying to find some means of highlighting the transparency, but I don't believe there would be a harm and I could actually highlight lots of potential benefits.

I'm not sure I understand. I'm going on Alessandro's axiom. I'm not sure I understand the question, so I'm not sure I can provide the best answer, but is the question whether if you provide meaningful consent, before doing all collection, there is no harm or -- I mean, is that essentially the question that we're asking, that you can't do harm if you've got meaningful consent?

MR. RACE-BRIN: I think that's what the question is asking, yes. If the user gives consent, then --

MR. INGIS: Okay. I think the answer to that is of course they can. Someone could always harm you with that information, and perhaps, we believe that those practices should be illegal. I mean, someone could still discriminate upon you based on the information that you

provided in a way that you think it's inappropriate. So I think the answer in that context is obviously yes.

I think there are sort of consumer harm questions. Now, there's a whole, obviously gray area that we spent a lot of time covering where, you know, it's not clear that there's that kind of direct harm. And of course, I believe in that context that a consumer, having given meaningful consent, yeah, obviously deserves the benefit of the doubt. Deserves to have their information used robustly and try to benefit from all these services that are being provided and the potentially new things that come from new data.

So I would say we would want to trust the consumer here. I think meaningful consent, obviously, can be a concept that can be somewhat difficult to quantify. But I think that's --

MS. RACE-BRIN: I mean, we did talk about the backstop of FIPPs and possible regulations, things like that, as kind of means for controlling exactly what you're talking about.

MR. ACQUISTI: Just to go back to the decision made earlier between privacy as a final good and privacy and an intermediate good. Example, subjectively, one person may not care and another person may care and that's totally fine. That's in your preferences.

Privacy is an intermediate good leading to specific benefits such as reduction in the cost needed to find a product or specific costs such as (indiscernible). These benefits and costs are completely independent of your subjective preferences.

MR. OHM: So we have about a minute, which means let's take three minutes to finish up. I'm going to ask you a question, but I'm going to give you one last opportunity to opine on anything that's been said as well. We're not going to give you a second round after this.

The question is this -- the question is should the agency, as it thinks about comprehensive data collection, think about the competitive landscape?

So should our assessment of any particular practice turn on competitive alternatives, lock-in, network effects? I'm guessing that most people would say yes, but elaborate on that. I mean, to what degree should that matter?

Commission Ohlhausen talked about we should have a level playing field. We shouldn’t be picking winners and losers. So what's the answer? Does competition or the lack therefore matter, as we think about this? And then also anything else you want to add. This is your last chance. I'll start with you again,

Lorrie.

MS. FAITH-CRANOR: Well, I think we found that competition in the privacy space hasn't really worked very well because it's so difficult for users to understand the privacy trade-off. So I don't think we should rely on competition as the answer is this space or probably any space when we deal with privacy.

MR. INGIS: I think we should make sure that the marketplace kind of picks winners or losers on products, event tied to data flows and that we should be careful not to pick a technology or some means of data collection or whoever's collecting the data to say geez, you shouldn't do it because you're in that particular role, more of the tech neutrality. And since we do get a chance to say something else, the one thing that I haven't mentioned, you've heard a tidbit of benefit here, but one of the things that I think we need as a business community or intending to do is to do a better job. You know, we heard a lot about harms, but do a better job explaining all the benefits.

One of the initiatives, and hopefully in future panels, we'll be able to do this is that the DMA has an initiative called the Data Driven Marketing Institute to really try and categorize a lot of the benefits because some of what's missing in the debate is well, we've

identified some harms. We've got some anecdotal benefits, but we really need to have much more detail if there's going to be policy decisions being made there.

MR. OHM: Alessandro.

MR. ACQUISTI: Well, competition and free market do not imply the absence of legislation. Legislation is what set the rules, the framework, the infrastructure, like the referee, which then keeps the players honest.

So we need both competition and the rules.

MR. OHM: Chris.

MR. CALABRESE: He stole mine. We haven't mentioned apps. I think they're an interesting marketplace where you may have a potential area to compete because people are sort of literally shopping for a type of software and downloading it one time and may be able to choose between things that -- if you can provide them meaningful clarity, you may actually be able to compete on something like privacy.

I will say that all of this needs to be underpinned by legal protections. I think if you listen to all the areas where we agree, try to make it tech neutral and pass some general legal prohibitions that are protections that are based on these areas of agreement, I think that establishes trust in the marketplace and I

think that benefits both consumers and industry.

MR. OHM: And for the last word, Mr. Hintze. I think competition clearly has a role. I mean, we have, in many cases, tried to compete on privacy. We run ads on privacy to make that a competitive issue. At the same time, if there are areas or situations where there's a lack of competition, I think that does go into the whole context question and what consumers expect. I think consumers would probably feel more uncomfortable with a company being very aggressive on data collection where they don't have realistic alternatives.

So I think it's an important issue. Like everything here, it's not the sole issue.

MR. OHM: So with that, I think we have another break 'til 3:15, but before we let you go to that, please join Katie and me in thanking the panelists for their participation.

(Applause.)

(Brief recess taken from 3:04 p.m. to 3:17 p.m.)

* * * * *

THE FUTURE OF COMPREHENSIVE DATA COLLECTION

MS. PARSON: Okay. We're going to go ahead and get started. Welcome back everyone. Please, don't forget, we are taking questions via Twitter at #ftcpriv. On Facebook, you can email datacollection@ftc.gov, and if you're in the audience, you can pass an index card to one of our staff and they'll bring it up to us.

This is our third and final panel of the day and we're going to talk about the future of comprehensive online data collection, which should just take a minute or two.

We're going to discuss potential next steps for industry and policymakers in this area. I'm Kandi Parsons, and attorney in the Division of Privacy and Identity Protection. My co-moderator is Chris Olsen, an assistant director in the division.

We're thrilled to have an expert group of individuals as our panelists today, so please let me introduce them.

First, we have Chris Hoofnagle, who is a director of the Information Privacy Program at the Berkley Center for Law and Technology, Berkley School of Law. Next to him is Randy Picker, professor of the University of Chicago Law School.

Next to him is Lisa Campbell, the deputy

commissioner of the Fair Business Practices Branch of Competition Bureau in Canada. Seated next to her is Jim Halpert, a partner at DLA Piper, and general counsel to the Internet Commerce Coalition.

Seated next to Jim is Alissa Cooper. She's a chief computer scientist for the Center for Democracy and Technology. And next to her is Tom Lenard, president and senior fellow of the Technology Policy Institute. And finally, Sid Stamm, lead privacy engineer at Mozilla.

Thank you all so much for being with us today. Chris, I'll start with you. In our March 2012 report, the Commission said comprehensive online data collection raised heightened privacy concerns and thus, warranted this workshop for unique consideration. Today we've heard a lot about the practice, so I'll cut right to it.

Were we correct? Does comprehensive online data collection, as we've discussed it, warrant unique consideration by industry and policymakers?

MR. HOOFNAGLE: Well, the definition, as stated by the Federal Trade Commission is the collection of data about all or most of consumer's online activities across multiple online locations. I think there are a number of things that are notable about this that have been elucidated from earlier panels. I'm sorry. It is on? Okay. Good.

One basic idea is that as companies collect more data, there is more risk of harm. I think we have to fully accept the idea that in a world of total information collection, we're going to have to get used to total security breaches. That's a problem that we often downplay and we don't consider very carefully in this type of data collection.

I think the other issue to think about is with comprehensive data collection, there is more likelihood -- it is likely more likelihood for uses that are unanticipated or unwanted by individuals. It's also very difficult for the user and regulators to detect changes in use.

One example that I like to use is Google's adoption of online behavioral advertising. If you look at the history of Google, the company used to critique OBA. It set itself apart from its competitors by saying that they didn't look at search history and it didn’t look at other data collected in internet sessions. But then Google switched policies and they did so silently. It was actually an analyst that discovered that Google had taken up OBA.

The other issue that I think is worth thinking about is the last part of the clause of all or most of a consumer's online activities. We heard some talk today

about people who have multiple connections to the internet. Focusing in more carefully on what we mean by all or most seems to be pretty important. Do we mean total and aggregate? Do we mean session-based? What about the problem that there will be linkages across these connections? And of course, we know that there are companies out there that are trying to link to have a single view of people's browsing experience across different networks.

Let me finally just mention that one tracking platform that has not been discussed much today -- it was mentioned by, I think, two speakers -- is mobile payments. I think mobile payments is going to be a huge opportunity for businesses to create a kind of unified view of the consumer and it will bring online tracking to the offline world.

You know, when you pay with a credit card today, there actually is some privacy in a transaction. It isn't a no privacy transaction. But when you move to many mobile payments systems, you're adding a new company to the transactions that learns the precise items that you purchased, in addition to where you shop and other information.

So mobile payments is one example of a platform that we have to think about very seriously, going

forward.

MS. PARSONS: Yeah, please weigh in. Tom.

MR. LENARD: Is this on or is this the -- yeah. Well, just a couple of things. One is that I think if -- and the question was the comprehensive data collectors, however they're defined, and it's still not clear to me exactly how they're defined. But in any event, do they warrant special treatment? I think we ought to be careful about kind of basing it on hypothetical harms that have yet to occur because the set of hypothetical harms can grow very large once you get into that. I think we really should base it on evidence of actual harms, if there is some. And I don't know that I've seen any of it and seen any systematic evidence of harms from comprehensive data collection.

I don't quite understand the argument that's been made that somehow, you know, why is 100 percent data collection worse than 80 percent data collection or 70 percent data collection. I think you can actually make the argument that -- I mean, if you look at it from the other side, from the benefits of data collection, and I think there are many benefits of data collection we should get in with, but one of the benefits of data collection is that you can more accurately serve your customers and provide what they want. Provide them

advertisements that are more useful.

If you look it that way then more data allows you to pinpoint their interests more accurately and that's a clear benefit.

MS. PARSONS: Lisa, do you want to weigh in on this?

MS. CAMPBELL: Yeah. Just picking up from what Chris said, I think there are three important points to think about it. The first is this, it's becoming difficult to distinguish between personal and non-personal data because even with best efforts to anonymize, data longevity and increases in data collection and store capacity make it increasingly difficult to truly and permanently de-identify anonymized data.

At the same time, it's increasingly easy to link pieces of data to a person's real identity. So the moment a piece of data has been connected to a person, any association between this person and virtual identity destroys anonymity of the latter.

We're walking around with super computers in our pockets and they have a geolocation capacity that in most cases is constantly activated and people just aren't aware of it. That's the first point.

The second point is we're all aware of how many

online business models are funded, but it's important to recall this on an elemental fact. All of the internet's free sites and services are funded by the collection of personal information, the mining of that data and advertising.

So put another way, underline the services we enjoy online and now a generation of people who have grown up to expect this is a complex ecosystem of trade and personal information. So there's a massive marketplace out there of data of individuals. It's of interest to marketers and advertisers, as well as employers, insurers, lenders, the government. And the plummeting cost of collecting and sharing this data and its utility as a financial underlay is something we can't discount.

I think on the point of special treatment and could everyone be treated alike, it's important to also think about the fact that there's a growing industry of companies who sole and main line of business involves mining an individual's personal data in order to sell it and provide useful analysis to advertisers. This all becomes more pronounced, of course, with Cloud computing.

The last point I think is important to keep in mind is the way we access the internet has changed dramatically in the last five years. It used to be

primarily via search engines and now it's increasingly through social networks and using the mobile devices I was talking about that had the geolocation capacity.

If you've looked at any of the studies in this area, we're actually biologically programmed to like to share information about ourselves and that tendency becomes even more pronounced in the online context. It just about doubles. So people really enjoy doing this. There's no sign that they're going to want to stop, and that is the primary starting for online.

If you look at the growth rates of some of the new startup social networks like Pinterest, Pinterest grew 5,000 percent and Instagram grew 17,000 percent between July of 2011 and 2012.

MS. PARSONS: Alissa, can you weigh in on Tom's contention that the harms of collecting closer to 100 percent of data are speculative?

MS. COOPER: Sure. So I think -- you know, it's been an interesting day here because we have, on the one hand, the conversation of what is comprehensive data collection? Have we defined it narrowly enough? Do people know what it is and on the other hand, even if we don't know exactly what it is, does it deserve protection? It's a difficult question to answer if you don't know exactly what the practice is, but I think, you

know, we've talked a lot about the economic harms. It's interesting to me that when we're thinking about -- we keep calling it comprehensive data collection, but we haven't really heard the word "surveillance," which is like, when you say surveillance, you know immediately, you have an intuitive feel for what that is, right. It's someone or some entity monitoring you, right. It's usually a public sector and not a private sector entity. But I think if you think of the practice, just think of what that term brings to mind, think there's a whole other dimension of this, which kind of gets to the reason of why did the FTC have this workshop? Why has it been called out separately, and that's because it invokes a sense of potential risk and creepiness and deterrence of particular behavior that online behavioral advertising and financial disclosures and other sector-specific activities don't necessarily bring up.

So I think there is something to be said for comprehensive data collection as a special set of practices, which is not to say they deserve some, you know, that we have to get into technology-specific protections, which I don't think would be the right way to go. I know a lot of people have said that here today. But I do think that just thinking about it through the lens of the word "surveillance" makes you realize that

yes, indeed, when just the fact of being monitored -- which we haven't even talked about what the data was used for yet, right, just the fact of having the data collected, does bring particular concerns to mind.

MR. OLSEN: Tom, if you want to respond to that first?

MR. LENARD: Yeah, just briefly. I don't necessarily think that's an illegitimate concern, but I guess I think it's an entirely different discussion that what we've been focusing on all day. I think we've been generally focusing on the collection of information for commercial purposes. There's a whole separate issue of a public sender and when the government should have access to this data, which I think it's a legitimate subject, but it's kind of an entirely different subject.

MS. COOPER: Sure. I guess what I'm saying is that I think part of what needs to be drilled down on here is from a consumer perspective, whether it's a public sender entity or a private sector entity clearly makes some difference, but how much of a difference is there and the sort of feelings that it invokes, maybe cross over a little bit from one to the other. And also that some of the data that gets collected by private sector entities does get into the hand of public sector entities. It's not like there's a stiff line between the

two.

MR. HALPERT: Well, first of all, it is important, I think, as Chris highlighted, to be clear on what we're talking about. Comprehensive data collection, if you really think about the meaning of the term "comprehensive," there is no entity, except perhaps providers of tool bars that are downloaded on multiple machines. It's really everywhere users are going on the internet and has a comprehensive picture of what's going on.

We heard earlier that many people access the internet from multiple locations during the course of the day, multiple service providers. They often use different browsers. There are opportunities for users to link up the information that, for example, favorites on different devices, but users should be informed of the implications of doing that. And the user has to take an affirmative action in order for that to happen.

There are sneakier ways that different entities can download tools to do this, but often those defy user expectations and can raise potential deceptive trade practice implications if they do so. So I think it’s important to distinguish what is truly comprehensive data collection from the snapshots in combinations of data. Even if you look at what Google is doing, there are many

sites that will not allow Google to collect information on the sites.

The information that Google is collecting is subject to the (indiscernible) for behavioral advertising is subject to the DAA opt-out. We can talk about whether the icon is sufficient or not, but there are tools well within the arsenals of even best practices to address what the vast majority of entities are doing here and whether it is something that is really a gross intrusion and is deceptive. The FTC has pursued quite a few cases in this area and I think will continue to do so.

It is true, also, that many communications are encrypted, and while there are certain ways to get around those barriers to reading the contents of communications, those can't be read. So I think we can talk in sort of a dramatic way about how there is a huge, huge, combination of data being collected, but ironically, it's not at the points of access to the internet where we're talking or even in the world of advertising. There can be other databases that are combined. Keep in mind that online data collections is one species of data collection, as we've heard in the initial presentation. There's a lot of offline data collection with often much more sensitive data and I think focusing solely on online data collection, saying there's a unique problem here and we

need to have a very, very different approach to this is not looking overall, even from a pure privacy perspective, quite apart from the benefits of advertising-supported content, for example, that Lisa discussed.

It's not really, I think, an appropriate public policy framework. We should look at this in the context of an overall collection and profile. This dystopia that we heard about on the previous about, you know, different sensors, Lorrie discussed, is truly a dystopia. Stu's ironic comment about that being awesome is obviously ironic.

We don't move toward that sort of world and it's very important that users, where there is comprehensive data collection, be given very, very clear information in an actionable point and be given the ability to object to and decide they don't want to be part of whatever the particular modes of collection are. But there is no single point of comprehensive data collection today. And I think we would all rule the day if there ever were that.

MS. PARSONS: Randy, I can see that you want to --

MR. PICKER: Yes. I guess we don't have a good sense of even the rules of engagement for single data

points. So it's hardly surprising that we're finding it difficult when we scale up and multiply by a billion.

So it turns out if you can see me, I'm not wearing a tie. And that turns out to be unusual in Washington. I don't think I own that data point. I don't think I have the right to control you from observing that fact. I don't think I have the right to control you from tweeting about it. Please do.

So I don't think we have a sense of what the rules of road are with the ability to observe data and then to draw inferences from it. Do you infer that I don't own any ties? No, actually, I own ties. Don't know how to tie? No, I can tie a tie. You should infirm a tenured a law professor who hasn't had to worry about clothing in a long time, that would be the right thing to say.

So then when we take that conflict, and the conflict is so powerful, switch it to the online context. So if Orbitz observes that I have a Macintosh, wants to draw inferences from that, that's no different than what happened in the old days when someone walked into the neighborhood store. So I don't think we have a good sense, even with the rules of engagement are for single pieces of data without saying, okay, let's multiply by pick your number and what happens when it's CDC instead.

MS. PARSONS: Talking about the rules of engagement, then, I'm going to turn to Sid. Let's assume that there are companies that are, as this morning, many of our panelists said there are companies that are not only capable, but some of which are tracking much of their consumer's data, even if it's not all consumer's data everywhere, at least their engagement with the consumer.

What should the rules of engagement be? What baseline standards, if we're going to move forward -- can industry adopt? Should policymakers consider? Should consumers consider? Sid, you're the one actually designing these products and services, so tell us what you think.

MR. STAMM: So this where I actually get to define what the future looks like, right?

First of all, I'd like to just kind of talk about how I feel the online world is quite a bit different than the physical world. One is I am wearing a tie, and you're welcome to tweet about that if you'd like, but if were online -- and this was an online -- well, it is an online thing.

MS. PARSONS: We are.

MR. STAMM: Okay. So for those of you who are online, maybe you've got some software running that's

analyzing me as I'm talking to you right now and it's observing a lot of things that an individual wouldn't observe, wouldn't remember and then probably couldn't fold into their reasoning about how to best sell something to me, how to best serve me, or how to best optimize how I interact with them.

So when we map how we work in the physical world to the online world, things get different because computers are fast and they know a lot of data. They can observe more quickly than individuals. I think, my hunch is, at least this is how I feel -- this is where the creepy factor comes from. Instead of just kind of defining how the world is going to look next year and what kind of framework we all have to subject ourselves to, I'd like to just kind of talk about how we've been approaching this at Mozilla.

At Mozilla, we're really focused on the individuals who are using the Web. We really are about them. Our mission is -- it's got laser focus on them -- making sure that everything we do serves them. So as we're developing our products, we've got this suite of privacy principles that we ask our engineers and our product managers and everybody else working on stuff to think about and to take into consideration and maybe use it to help them design their product with privacy in it.

Let me see if I can reorganize those words again. Do privacy by design or something like that.

We found that whether or not these principles are recorded in any sort of written fashion or brought up specifically or addressed individually, as long as we're focused on the individual, these surface automatically. So the first principle we kind of follow as we're making new products or refining ours, there are no surprises.

I think this is one that a lot of people will agree with, that the things we make for these individual consumers should not surprise them how they operate. If they find out that we're collecting some data, it shouldn't surprise them that we're collecting that data. So if we're building something that will surprise them, surprise a reasonable person, we might be doing something a little weird.

This jives with the way we've been talking about being consistent with the context of a transaction, to me. I don't know if it's a one-to-one map, but that sounds kinds of similar. Basically, the way Mozilla is mapping that onto our operation is that we're going to collect data if it's for the purposes that the user is requesting. Anything else is going to be pretty much like a surprise.

The second thing that we really kind of focus

on is real choices. When possible, people should have a choice. They shouldn't have to not use Firefox because they disagree with the fact that we don’t use rounded rectangles or something like that, which isn't true. I think we do rounded rectangles, but I'm not exactly sure.

But the point of real choice is to educate consumers at the point of collection or where it's relevant and that's the key. Not just inform, but educate. They have to understand it if they can make a choice. Otherwise it’s a dialogue box with a big whatever button and nobody really understands what’s going on. They're focused on sharing something on their Facebook wall and they just want to get it done.

The third one is sensible settings. This is the defaults. This is kind of the Holy Grail of security and privacy. Things should just be secure and private by default and we should have all of the valued consumer and to businesses. You know, everybody lives happily ever after. Real choices exist because you can't always satisfy all of the people all of the time. So sometimes there has to be variations in how the software operates.

But the sensible settings is a balancing act between the user's experience doing what they want and keeping them safe and keeping them in control of their data and the data they generate.

The fourth principle that we kind of focus on is limited data. So as we're building products, we try our best to make sure that we collect what we need to give the consumer what we're offering them and that's it. If we don't need extra data, it feels to me like a liability. Some people who want to do experiments may feel differently, but if we're focused on providing an authentication system, we don’t need to know things like all of the websites you visited and how often you visited them, only the ones that you've logged into with this authentication system.

Finally, the fifth one is user control. This is kind of the essence of all of these. We think that people should have an understanding and choice and control over how their data is used online. So wherever possible, we enable our users of our products to be in control of how their data is shared and with whom. It's not, I'm sharing with people that I'm friends with on Facebook and the rest of the world also gets to see it. I'm sharing and I understand with whom I'm sharing it and how it's going to be shared.

We have a sixth principle as well, but it's just extending these five onto our business partnerships. I think this probably won't work for everybody because not everybody is focused on consumers or the people who

are using Firefox, for instance. Although, I'd would be really cool if everybody liked everybody who was using Firefox. But I think it's a good start and I think it's something we've tried and we've been successful at employing in our engineering efforts in our products. So I hope that helps a little bit.

MS. PARSONS: You play into the happily ever after future. It sounds like it works for everybody.

MR. STAMM: Unicorns and rainbows.

MS. PARSONS: Jim, can you weigh in on, to a certain extent those principles, but whether traditional approaches, such as notice and choice or the FTC's proposed, or now final framework, work in this space or if we need to consider more with the comprehensive collection.

MR. HALPERT: Thanks. I think, first of all, what Mozilla has done is admirable and we heard earlier from Microsoft about their thoughts. You could hear from many other companies who take privacy by design very seriously. I think when we think about the notice in choice framework here, it's important that consumers actually read the notice and that it be placed in a way that's conspicuous if there's going to be a gross an enormous collection of data that consumers might not otherwise know about, so that you don’t have data

collection running in the background. But it's important also to be realistic about which entities are in a position to provide that sort of notice. It may not be possible for every entity to provide a pop-up screen on a user's device, but it's certainly true if you look at, for example, the unsuccessful deep packet inspection trials. Those came to light in the United States because service providers provided prominent notice and at least found out what was going on.

So I think when you look at frameworks, if you do require notice and you do give consumers the ability to say I don't want to be tracked, for example. You do have a situation in which even if there is only one service provider for a particular service, you don't have consumers choices being overridden as a result of a take it or leave it sort of offer of the sort that Commissioner Brill spoke about earlier today.

MS. PARSONS: I just want to do a quick follow-up. On the previous panel, Lorrie and Alessandro both spoke to some of the challenges with respect to notice. Can you speak to how those play into informing consumers, what the solution to that could be?

MR. HALPERT: Sure. I don't think -- both Lorrie and Alessandro have done important work and I don't think that either shows that notice is impossible,

but it shows that it's important, for example, to provide just in time notice and what that is in the context of universal data collection. It doesn't makes sense to, as Lorrie explained it, provide notice all the time, but just in time notice is very important so that the consumers are informed at the point at which they're making a decision about whether to proceed or whether to allow or opt-out of whatever the frame is, the particular type of collection.

In terms of Alessandro's point, it reinforced Lorrie's point about data uses not being properly understood. That points to using easy to understand, plain language. Not using legal ease. If there was an icon to have a way to easily explain what the significant of the icon is and in a way that individuals will understand, but I don't think that that research says you throw notice out the window and decide not to use it. Also, you have uses, for example, for network security purposes, for example, that are pretty vitally important. You can't just say no, don’t do it. Don’t use the data for security purposes. So we have to come up with a way to make very, very heavy collection of information transparent to users so that they understand and can make decisions.

MS. PARSONS: I'll get to each of you in turn,

but I do want to turn to Alissa because you have chatted about the different ways in which certain of these types of entities may struggle to properly inform their consumers, such as ISPs or operating systems that are maybe running underneath. Can you speak to that?

MS. COOPER: Sure. Actually, funny that you bring up those notice. Jim, I think we've both been out of the country for a couple of years since NebuAd was selling its services in the U.S. But what I remember from that incident is that the companies sent notices to their consumers that didn't actually explain what they were doing. They said that they were going to provide this great benefit to their customer in the form of third-party advertising. What got the information out about what was actually going on was a couple of congressional hearings.

So I would actually say that there are definitely still challenges that remain and that's just a matter of what the actual content of the notice is, right. I think companies have found it difficult to explain the actual value proposition in terms of what's going here. I read a few privacy policies in the run up to this particular event and I, myself, found it difficult to really determine what exact information is being collected by particular carriers for specific

purposes. How long it's retained. I didn't see a whole lot of retention limits disclosed anywhere and which kinds of data or which are used for which purposes.

I think it's very sort of attractive to say we need all this data for security, and therefore, we're going to use it for a bunch of other things too because we have to have it. I think even a security rationale sort of demands more. Demands of retention limit. Demands, knowing how long data is kept in what form and which data is being collected for that purpose. And then if it's going to be used for other purposes, then those need to be disclosed as well.

Just one other aspect there because I think, Sid, you know, you said that your set of principles, you're not sure if they apply to everyone. I mean, to me, they sound like why not? Why couldn’t they? They sort of sound like a bit of a spin one many of the FIPPs. So it seems to me that they would be appropriate in lots of other situations.

I think, particularly, the one that jumped out at me that you mentioned was real choice. You said that people shouldn't have to not use Firefox if they don’t like a particular aspect, especially with regard to the privacy aspect. I think that's a fantastic rule. I think I shouldn't have to change my mobile carrier or my

ISP or my operating system or my browser just to get out of comprehensive data collection. To me, that seems like a reasonable baseline rule. So why not take something has done well and extend it a little bit further.

MS. PARSONS: Okay. I'm going to let Tom weigh in and then we'll go down the line and then we'll come back.

MR. LENARD: Thanks. You know, I think it would be useful for the FTC -- it seems to me that don't really have a baseline of what actually is going on out there. We talk about whether we should require these things, but I suspect that certainly most major websites are already doing them.

Between 1998, for those of us who are old enough to have been working in this field a relatively long time -- but between 1998 and 2001, there were four annual studies done by the FTC, as well as other people, basically just gathering facts. The one that I was involved in, which was the last one in 2001, we looked at the 100 most popular website and a random sample of the rest of the websites and just gathered information on what their privacy practices were so that we knew what was going on. I don't think there's been a study like that done since 2001. It's obviously a long time in internet time.

MS. PARSONS: Sid, did you want to weigh in?

MR. STAMM: Yeah. I actually want to come back to the notice and choice discussion a little bit more. Notices are hard. They're necessary, but they're really hard to get right. One of the reasons that they're harder, especially with comprehensive data collection is that we found Firefox users, and I would imagine anybody else who is browsing the Web, is really focused on one task at a time. They're really focused on doing one thing. They want to read their email. They want to go buy that new espresso maker because they need more espresso and theirs is broken.

They want to do one thing, and if they go to a website and they get a notice about something that's completely orthogonal to the task at hand, they're far less likely to first, read it, and second, understand it because they are so focused on that espresso machine. So that's why it gets harder. Notice and allowing choice at the point of collection is good, but we found that notice and choice, when it's related to the task, is significantly better.

MS. PARSONS: Okay. So we're going to come back to the concept of information that Tom brought up a little bit later, but I want to drill down a little bit more on what should guide our standards. We've discussed

notice and choice, but earlier today we heard a lot about uses and harms. So I just want the panelists to take some time to discuss uses that may be particularly pernicious and that we should consider whether comprehensive online data collection should be used for those at all and whether we should focus exclusive on harms or if that's the wrong framework.

Chris, would you like to start on that?

MR. HOOFNAGLE: I'm not ready to consider the use question, but as to harm, I think a lot of our conversation today assumed that the only value we were pursuing is increases of efficiency and this idea that there is utility and greater targeting, and more targeting equals more utility, period.

I want to just pushback to say that there might be utility to individuals and to our society through having privacy, having more space to play, as Julie Cohen put wrote in her recent book. For those of you who are firmly in the harm camp, it's worthwhile picking up Julie Cohen's book and thinking about the ways in which providing people space to be away from surveillance -- because I think Alissa is right, this is surveillance. Allows our society to be dynamic. If our end policy goal is efficiency and we can only state policy goals as increasing utility for advertisers, we are in real

trouble as humans. I think we should be able to express, from a policy perspective, that we have preferences that sometimes will make advertising less efficient or reduce utility for advertisers.

MS. PARSONS: Please, go ahead.

MR. PICKER: So this amazing ecosystem that we all take great pleasure in every day, has sprung up and it's been free. And it has done that largely free of government regulation. So much of the discussion today is acted as if this privacy by design principle imposed, what I think of is only a Soviet style that comes at no cost. And this innovation that has sprung up has been a remarkable achievement in the face of dominant firms. So part of what we have to focus on is people should be free to use Mozilla. And if Mozilla wants to go down that path, God love them for doing that. That will make it possible for you to go ahead and play and do all the things you want to do. I'm all in favor of play and privacy and redefinition of itself, but at the same time, we have to be aware of the potential cost of imposing.

Have you read the media guidelines, the Smart phone app guidelines that the FTC has put out? They're not long. It's eight pages long, so you can read them. I think they expect 14-year-olds, who are building apps, to read them and do privacy by design. I think we should

be concerned that the next generation of innovators are going to be turned into lawyers. And I love lawyers. We probably got enough of them.

MS. PARSONS: On this question, the question of should we be looking at uses, harms. Earlier today Ashkan talked about low amounts of sensitive information versus high amounts of nonsensitive information. I would like to just go down the panel and have each of you weigh in on these particular concepts in driving our standards. Should they be harm-based? Should they be use-based? If you care to. Lisa.

MS. CAMPBELL: Look, I'm actually a big fan of open data. We've seen the great innovations, to your point, Randy, of the things that can happen when innovator and creators can have access to valuable public data and all sorts of useful applications can arise. You see it, in Canada at least, particularly at the municipal level, all sorts of really useful services and applications have sprung up.

So I hear what you're saying about that, but I think we also have to be mindful of -- you're right; the basis of internet explosion of services has been -- the trade has been give us your personal information and you will get this service. I don’t know that we're saying that that shouldn't happen. I think the comment that

we're saying is be aware that it is surveillance. Be aware that there are public actors and private sector actors this space. Consumers seem largely unaware and perhaps, it's just more transparency, more consumer empowerment that needs to happen to balance things out a little.

MR. HALPERT: I'd add that this issue is not uncomplicated if you think about some of the embarrassment of sense of health information and that sort of thing coming to light. But it's extraordinarily difficult, in my mind, to draw a line between, on the one hand, a truly comprehensive sort of data collection and what's a lot of data collection. How do draw that from a policymaker's perspective. I think in the end, to avoid a different form of arbitrary discrimination in a regulatory regime, it probably would make sense to -- yes, to prohibit certain forms of discrimination and the example of the DAA eligibility screening principles with regard to information that was collected for behavioral advertising is one example of that. And then for very, very large forms of collection of information to give users choice as to secondary uses of collection of information. it's also worth considering whether the information is stored in a way that it readily identifiable or not identifiable without an unusually

large amount of effort. I can see Paul beginning to look at me a little bit funny, but maybe he agrees. I don't know.

I think that these are the sort of lines we should think about, but in general, we're talking about barring objectionable uses and then giving some degrees of clear transparency to users and degrees of control over secondary uses.

MS. COOPER: I don’t know that I have a lot of clear answers on this one. I think my take away from listening to folks talk today is that part of the reason why this is so difficult because you have, on the one hand, massive economic benefit and massive social benefit. And on the other hand, you have potentially massive social harm and social cost and personal cost, and quantifying those things is impossible. There are some things that you can try to quantify and I think there are lots of those aspects today that we talked about that haven’t been thoroughly quantified yet and maybe could be. Deciding how you're going to strike that balance is a very difficult task, which is why I think we often doing a case-by-case evaluation. Why you wait until you can identify a practice in the marketplace before you decide to, you know, if you're the regulator to bring a case or if you're an observer to bring it to

the public light or whatever you might do.

So I hesitate to try to provide some prescription that could be used to set any particular policy because I think it's really difficult to do that without a very specific context where you can actually try to weigh the benefits against the risks.

MR. LENARD: Well, first of all, I'd like to kind of second what Randy and some others have said in term of the -- I mean, I do think privacy policy is kind of a major innovation policy and we should look at it as a innovation policy because it really, virtually all of the innovation on the internet depends on, in one way or the other, the collection of information, either to develop the product, to improve the product or to provide the funding for it. So I think it really needs to be looked at in that context.

Now, I approach the subject basically in terms of sort of nonsensitive information. I'm not talking about medical information or financial information, I'm talking about the use of information for other commercial purposes online. And there, I do think it has to be harm-based. Harms can be broadly defined, but I think it needs to be something more than just a collection of the information, per se, as a harm because -- I don't know. I guess I think it needs to be something more than that.

Listening to the discussion today, I mean, I think people get a lot of mileage out of the Target example about the pregnant woman. I'm sure we're going to hear that example for the next five years, but it is an anecdote. It's somewhat of a novelist situation and I think there needs to be more systematic evidence of harms before doing something.

MR. STAMM: So I'm kind of thinking along the same lines as Alissa here. I don’t really have any sort of prescriptive advice, but I want to dig into why this is such a hard thing to reason about and go back to my example about tweeting about the fact that I'm wearing a tie or that other panelists may or may not be.

One of the big problems is that people's mental models of how they interact with other entities, other people in the physical world doesn't map directly to the online world because a lot of the actors in the online world are invisible. Users don't perceive them. So there's this gap between what people think is going on and what's going on and that causes surprises and that causes angst and the creepiness factor.

There is concept of civil inattention that I've heard Dana Boyd talk about, and a couple of others as well, but the idea is I'm walking down the street and I don’t latch onto a bunch of people and just start writing

down everything that they do. Part of the reason is that it's impractical, right, to do that. It wastes a lot of my time.

The other part of the reason is it's kind of creepy. So I participate in civil inattention and I don't remember the things that I've seen them doing or what they're wearing as they walk down the street. This doesn't occur as frequently online, but people expect it to happen because this is how they interact with others in the real world. This is one of the reasons it's so hard to reason about what's actually wrong here. It may not be I can no longer buy ties because I didn't wear one on a specific day or something like that, but the problems are maybe not as easy to quantify as a harm.

MR. OLSEN: Can I follow-up on the harm point? Ashkan, this morning mentioned a hypothetical example of a hotel that hosted very scandalous activities and there was a harm discussion about that. We actually have a real world example, not of the hotel. I see you laughing about the hotel, but there is a hotel in New York that fits that model, but we had a case --

MR. HALPERT: Computer company.

MR. OLSEN: -- involving a company that rented computers. Rent-owned stores rented these computers. The computers were capable of remotely activating the

webcams. The rent-owned stored could activate the webcams. They could trace the location of the computers, ostensibly, to recover the computers in case payment was not forthcoming. The consumers were not told about the remote activation capabilities. The webcams were, in fact, remotely activated and people were observed in very sensitive, delicate situations. I think everybody in the room would have a real problem with that.

The question, though, becomes is that harm in a legal test. There are two questions. 1) Is that harm if people know about it? If the consumers themselves find out that they've been videotaped. Or is there harm if consumers are not aware of it at all? If the tree falls in the forest and no one hears it, does it make a sound? If the webcam is being activated, the data is not being used at all. Individuals are being observed by the rent-owned stores. Data is not being sold or shared. Consumers never hear about it. Is there harm?

Anybody can jump in.

MS. PARSONS: Why is this a useful question?

MR. OLSEN: Well, I think it gets at the point of is there actually a debate about harm? Shouldn't we accept the fact that harm can occur merely by the collection of sensitive data in certain circumstances. Not by uses alone, not by sharing of data, not by actual

measurable impacts on individuals.

MR. HALPERT: Well, I'll respond to that from a legal perspective, but also from a kind of common sense perspective. There is an extensive body of state law about what constitutes an invasive use of videoing technology. Places like changing rooms, bedrooms, and bathrooms are all traditionally considered to be true zones of privacy.

The example of a computer being placed in somebody's home without the individual knowing, and in some cases, people actually having been videoed naked without their knowledge, is a very traditional notion of a privacy harm. It’s an intrusion upon seclusion. So I don’t think that this hypothetical is all that applicable to a more complicated world of users going to getting very valuable web content for free, essentially, on the internet in this marketplace that Lisa described, where there is a fair amount that is going on, at least that's being made public to a fair number of people. So I don’t think that this hypothetical really addresses the more complicated -- I'm not saying uncomplicated, but the much more complicated world of data collection and tracking that's occurring on the internet in areas that are essentially public, most of them.

MS. PARSONS: Chris, do you want to weigh in on

this potential analogy if pernicious or comprehensive data collection can make us unwittingly naked online?

MR. HOOFNAGLE: Not exactly. What I want to say is that Chris's question and Ashkan's earlier discussion of this is profound in that it's asking us why do we think this is a privacy problem.

Perhaps in thinking about why it is a privacy problem, we can elucidate other activities that we also think is privacy invasive. This is kind of a larger point, but the focus on harm is taking away our decision-making ability to say -- to determine the society we want to live in. It's undemocratic.

We're basically moving the goalpost to the point where unless you can show economic injury -- and that is the argument that these companies make in litigation -- there is no standing. You can't go to court. So this harm discussion is robbing us of the choice to democratically say that we find it objectionable to put a camera in our bedroom or to spy on us as we traverse the Web.

MR. OLSEN: Let me build on that and take it out of this Designer Wear, which was the name of the case, scenario, and talk more about --

MR. HALPERT: It's an ironic name, Designer Wear, but anyway.

MR. OLSEN: Right. I want to talk more about the information asymmetry because that's, I think, in part, the issue that I was getting at and, in part, the issue Chris raised. There are more and more companies able to collect different data points and it seems like that is the way the competition is moving. Apple and Google and Microsoft are attempting to capture multiple different data points through tablets, through mobile devices, through the desktop and attempting to collect as much consumer data as possible. The question is, is there an information asymmetry there that consumers know -- we heard a lot about this this morning. Do consumers know about the scope of that data collection so that they're able to make the sort of choices that Sid talked about, the informed choices and they understand the bargain? That's really the question. It was no possibility for the consumers in Designer Wear to make those choices. And is there a possibility for consumers to make that in other contexts?

I think Stu Ingis talked about the DAA icon. That evolved, in part, because there was an information asymmetry. People did not understand online behavioral advertising. Industry stepped in to address that asymmetry. Is there a similar asymmetry in the correlation at different data points?

MR. HALPERT: I think the question is to what extent you want the government to engage in regulation of a design of these products. What I think I heard Alissa say, basically is that she thinks she should have the right to use Firefox in a particular mode, and I don't want to put words in your mouth, but the government, if necessary, should regulate that. Try Google.

Google obviously offers an interesting range of products where they try to induce you into, as it were, providing identity information to them. Should we regulate that? When my computer is on, Google has my identity. Why? Because I use Google Reader. I use RSS feeds. That's the only way to make that system work. I accept what goes with that. I could opt out of that, but I wouldn't get the benefits of that service. Should we require them to organize that different somehow? I think that's the question with regard to regulation or whether you think we're going to have a dozen browsers -- that's what the EU thinks is out there, a dozen browsers -- and will let the market choose and let consumers choose, like Alissa, which browser they want to use.

MR. OLSEN: I think you wanted to respond, Alissa.

MS. COOPER: Yeah. So I think I'll give you the counter example, which is my fixed line broadband

provider. Should I be able to use the internet in my home over a fixed connection without having the url of every website that I visit retained indefinitely.

MR. OLSEN: So what's your number is my question. That’s what I always ask at this point?

MS. COOPER: Number of what?

MR. OLSEN: How many competitors do you think you need to have in the marketplace before you decide you say it's not an issue?

If 12 is good on browsers and two is insufficient on landline, what's your number?

MS. COOPER: There's no prospect of reaching a reasonable number in the U.S. anytime soon. So it's good that we're having this conversation right now.

MR. HALPERT: Turning to reality, ISPs --

MR. OLSEN: I don’t know what that means.

MR. HALPERT: No, just the facts of ISP's retention of weblogs. ISPs have kept weblogs for more than 15 -- I mean, since the ISP industry in the United States. It has never been considered comprehensive data collection until these NebuAd trials raised concerns. It's important to know that most ISPs decided -- and I advised a number of them -- decided not to do those trials because of the importance of their customer relationships and because of a variety of different legal

issues that are raised by form or NebuAd.

So it never went to the point of being the subject of this hearing. It's important to know that -- one service provider that was mentioned earlier never actually ran the trial. It was an announcement. They announced in Ed Markey's congressional district -- probably not the best idea -- and they immediately turned tail and pulled back. But it's just to show that they are clearly restraints on ISPs, and many ISPs decide not to go forward with those sorts of models.

And finally, in terms of how long the information is kept, there has been congressional hearings where members of congress have beat very, very hard on ISPs, demanding that they keep logs longer in order to facilitate investigations of child pornography. So in a world where the ISP is sort of being pushed back and forth, as though they're consciously deciding to keep this information for as long as they possibly can in order to innovate or market or do anything with it, they really are in the middle and their core business is providing service to consumers.

They need to keep certain information in order to secure their networks against Malware, against hacking and then they have these pressures from law enforcement. To be shot at from both sides, I guess, may mean that

they're doing the right thing, but this is not a situation where weblogs are the future of comprehensive data collection. They are very much a long-standing practice.

ISPs networks are configured in different ways and sometimes they can have more information flowing through them and sometimes they can have less, but to single out the ISPs that are doing far, far less of this than a host of players on the internet and a host of entities offline that are in the business of selling information about consumers to third parties doesn't make a lot of sense to me.

MR. OLSEN: Lisa, you wanted to weigh in?

MS. CAMPBELL: Yeah. I have just two points around consumer choice. So the most common model is notice and choice, but the general consensus seems to be that notices aren't read and they give regulators the chance for light-headed oversight of emerging markets. Companies have the option to look like they're complying, but in reality, I think we all agree that it fails to protect consumers because it relies on theoretical knowledge as opposed to practical knowledge that they can act upon.

I would suggest that we probably haven’t done enough to explore the potential of notice, especially in

the mobile environment. What we've done is taken the written form of lengthy notices and just tried to continuously adapt it to the mobile environment. Even a lot of Twitter notices, you'll still see rely on the written word. What notices could be to be more effective is more experiential.

Some scholars have talked about the use of a shutter sound when you have an app that takes your picture. So using sound, touch, well-recognized images could actually be more effective quicker. That's something that could be explored more. The second point, though, around choice, perhaps beyond that, privacy regulators in the main who have adopted sort of an exhortation to best practices or alternatively, shame and blame approach with companies that violate privacy regulations. Perhaps they need to consider better promotion and education of tools to regain control over one's personal information and steps to anonymize data, you know, empowering people to actually make real choices.

So the question for policymakers then becomes is access to viable cryptographic software an indication that someone has something to hide or that they just want to be able to participate online with some privacy?

MR. OLSEN: So Tom and then Chris.

MR. LENARD: Yeah. This discussion of ISPs I think is somewhat along the lines of earlier discussions where there seems to be this assumption that companies don't care what their customers think. Actually, customers do care of what their -- even big companies care about what their customers think. People switch ISPs all the time, for reasons of price, speed, the ISPs. Even with two -- and this is not the place to get into detailed discussion of the competitive structure of the ISP sector, but I think it's more competitive than that.

If these companies thought they could get a competitive advantage on the basis of privacy policy, they would. I think the reason that we don't observe it is because most of their customers just don't care. They don’t see any harm in what's going on.

MR. OLSEN: Doesn't that go back to the information asymmetry point, though? If they're not aware of what's going on, are they able to make those choices?

MR. LENARD: Listen, consumers are not going to understand what Dan Wallach said this morning. I mean, what's the level of understanding they're supposed to have? I think consumers understand the rough bargain they're making, in terms of trading their information for content, useful advertising, fraud protection, et cetera,

a whole bunch of services. They don't understand all the details of how it works and it's pretty complicated of how it works.

MR. HOOFNAGLE: I think it's hard to come to the conclusion that people don't care. We have to keep in mind that people are social. But as Sid pointed out, the Web is an asocial place. When we use the Web, we bring to it our assumptions about the world, assumptions that people will act in certain ways.

One of the interesting things about Alan Westin's research, over decades, is he asked consumers whether they thought that businesses handled information in a responsible and confidential way. Year after year he found that more than 50 percent of Americans believed this.

My research, and we've done three large-scale surveys of consumers on privacy, suggests something very similar. That people think that the companies they do business with are actually acting in a fiduciary role and they believe that those companies cannot sell data to third parties. Perversely, they believe that if a privacy policy -- if a website merely has a privacy policy, it means that the website cannot sell data to third parties and it means that one has a right to delete data, and it means that individuals can sue that website.

You say people don't care. I would asks us to remember -- I would remind you of the Do Not Call situation here. The DMA ran a telemarketing Do Not Call list. They call it a telephone preference service for a long time. And at its height, it had about 4 million enrollments in it. I think you might have been able to say well, people just don't care. They don't enroll in this thing. But when the Federal Trade Commission gave people an easy to use simple choice to opt out of telemarketing, people rushed to it. There are 217 million enrollments in the FTC's Do Not Call database.

If we give people information and the ability to make choices, I think they're going to run to them. What this debate is about, if you really dig deeply, is the fear of giving people such choices.

MR. PICKER: I emphatically reject that assumption. I think it was assumed in Tom's statement and people responding to it, but I can tell you that any large internet company with a first-party customer relationship knows that its customers care. Thinks carefully and vets its uses of personal information, as we've headed toward the end of the last decade into this decade, carefully. And are not going to go running, selling information in all sorts of wild ways that users wouldn't expect.

I would also point out that there is a huge cottage industry of privacy class actions in the United States. And generally, the companies that get sued and the companies that are the subject of FTC enforcement actions are companies that do very -- highly unexpected things with regard to consumer data, often more sensitive consumer data, and fail to disclose those activities.

If you look at a series of the whole "What They Know" series in the Wall Street Journal, it's been remarkably successful in bringing to light unexpected uses of consumer data with significant negative consequences. Looking at this, you can point to small players and say they don't play by the same rules, but I think we have an awakening in the United States as to the importance of consumer privacy that extends beyond first-party entities because first-party entities that have contracts with third-party entities are starting to require them to take strong privacy measures. So I think we're seeing a significant culture change on the internet and a greater thought about how information is being used.

Yes, you can point to incidents like the pregnancy incident to show that companies are making mistakes, but there are first-party constraints here that I think this discussion is not recognizing.

MR. OLSEN: Let me jump in. Go ahead, Chris. Quickly.

MR. HOOFNAGLE: Why was it a mistake? I mean, we heard from Howard Beales earlier that knowing can't be the harm. So what was the mistake that Target engaged in by knowing that this woman was pregnant?

MR. HALPERT: It's information that one infers about people's health conditions and it is in a somewhat different category than what somebody is willing to pay to buy a car or whether they're likely to want a car and there's a different sort of sensitivity associated with it.

MR. LENARD: I didn't really mean to say that these big companies -- that nobody cares. I want to amend that. I mean, I think these big companies do care about their customers and they care about their reputations and if there is a privacy glitch, you know, they want to avoid it because they know they --

MR. OLSEN: Well, let's talk about that a bit because that raises the point of transaction cost and potential market imbalance. This is a subject that Neil Richards touched on this morning. To the extent that there are companies out here, large first-party companies who are able to gather together multiple touch point.

Obviously, there are consumer benefits with

being able to have your services provided across different devices and in different places, but does that not also create transaction costs, in terms of your ability to switch services? And does it create an opportunity for a large first-party to push the envelope to innovate, to do things like the Targets in the area that is perhaps, in a murky area and not risk losing customers because there is a locked in effect?

MR. HALPERT: If notice and choice is offered and the notice is reasonably clear so consumers understand what they're deciding, then there is no asymmetry of power and users have a choice as to what's occurring. One can go to opt-out centers and opt out. One can decide whether or not to use a signed in -- to sign in on Google and have all one's surfing activities be run through the Google sign in.

One can decide whether or not to download different apps on different devices and link them. There are a series of choices that are available today. We can talk about whether information should be clearer to consumers so and choices to opt out should be clearer, but the notion that there is a world where consumers are powerless today and there is an ever increasing market power by these players that a diversifying and innovating and offering different services to consumers and also

using data in order to innovate more, I think is an oversimplification of what's going on.

MR. OLSEN: Sid, did you want to jump in here?

MR. STAMM: Well, I think there is a "what if" there that is kind of important to talk about and whether this notice is effective.

MR. HALPERT: Right. But that's really the discussion. It's not do consumers not have choices and is there an asymmetry of power. There may be issues about how clear a notice should be. Most of my law practice involves counseling clients on privacy compliance, but I think that's an issue about how to write notices better. There's research that I think was aired today that can significantly help with that. But that's the issue. It's not whether or not consumers really lack market power in the face of an overwhelming coercion from market power.

MR. STAMM: I think there's also a situation where I may be interacting with one company online and so are all the people that I want to communicate with and the only way that I can communicate with them is through that one company. I may not like this company, but I have a choice to make and it's not whether or not to use this company. It's whether or not to participate with my friends.

MR. HALPERT: I actually think that if one doesn't like a particular service, there are a variety of technology tools to use. One can also find the email addresses of your friends or suggest that you move to a different social networking site that is more to your liking. I don't think you're without ways -- I know people who break Facebook's sign-on rule. They create a fictional identity and then communicate with their friends, not in their real name. It violates the terms of use, but people find ways to do that.

MR. STAMM: I want to be a good Web citizen and not violate terms of use. And I want to communicate with my friends who only spend time on this one social network.

MR. HALPERT: Well, if they're your good friends, you can talk to them about going some other places.

MS. COOPER: One thought there is that I think this conversation really needs to gel with what Alessandro was talking about, which was about your subjective, ex-anti preferences, not necessarily matching to your ex-post feelings about your choice. I think network effects are one way that throws a wrench in there.

I think there are other sort of aspects of

lock-in that can be really important if you sign a contract for two years or you buy a device that you can't take to a different network or if you just have your sort of run of the mill, sort of status quo bias.

There are reasons why you don't want to leave a particular service and then there are countervailing reasons that you find out afterward, after you've already kind of bought in that make you feel like you do. To me, that's why the full set of FIPPs are so important because then you have to ask, well, what are the other protections there that are helping to serve you. Is data being identified? Is it not being shared broadly? Is it being deleted after the period of use?

That's why all of those after the fact protections are so important because you will get plenty of consumers who, I think, end up in that situation where they fell like they can't leave for other reasons, even though the privacy aspect makes them uncomfortable. I think that's why just relying on notice and choice, you know, if you don’t have a choice, it's not really adequate.

MR. HALPERT: I agree that there are firm information practices that can be helpful here, but I think it's also important to recognize that there is significant innovation that involves use of data if data

is the identifier, to the extent that it's difficult, if not technically impossible to reidentify it. I can be used for enormously beneficial innovative purposes.

We're talking about the most innovative portion of the American economy that offers consumers enormous amounts of services and content at no charge. And it's important to balance the innovation and the social goods with the privacy -- within the privacy concerns of consumers, but not to assume that the default has to be never share and not to assume that the default has to be destroy all data if it's technically possible for somebody with enormous computing power to reidentify it.

There is a very important economic implications of how one regulates privacy on the internet today and it's important to proceed cautiously and to proceed, where possible, through self-regulation and through higher level principles, rather highly-specific statutory and regulatory --

MR. OLSEN: I want to follow-up on the point about FIPPs. This gets at an issue that has come up on the panel, in terms of competition. There are already sectorial laws in place that govern certain industries, in terms of privacy.

Arguably, there is already a potential imbalance. There is the Cable Privacy Act. There are

the CPMI laws. There are companies who will argue that they're not able to do what other companies in this space are able to do and that begs the question, is the answer to that problem a more general set of rules, or principles, or standards that would apply across the board.

Alissa, do you want to address that?

MS. COOPER: Yes.

(Laughter.)

MR. OLSEN: You find this a relevant question?

MS. COOPER: This is a very relevant question. No, I mean, I think if we can go back to the beginning and have a baseline law instead of sectorial laws, then the problem you just articulated wouldn't exist.

MR. OLSEN: Lisa.

MS. CAMPBELL: I'm also like Alissa, glad you asked that question because if you look at what's going on in jurisdictions around the world, banks and mobile network operators are entering into partnerships to create mobile payment systems, to the point that Chris made. I think that issue and that development is going to crystallize a lot of what we've talked about today.

In other jurisdictions, telecommunication companies are buying financial institutions and conversely, banks are buying telecommunications companies

to be part of the game of mobile payments. Two trends are forging, I'd suggest, a link between competition about our trust issues and privacy. The first is what we've talked about on this panel, the economics of online advertising and the way goods and services are monetized.

And then secondly, the rise in what you can largely call internet intermediaries. So search engines, social media companies, ISPs and their use of information about consumers that flows continuously to them as part of the services they render. Just to pick up on what we've talked about, everybody knows, I think, or has heard of the square wallet app for Starbucks. It's a huge convenience factor to pay for a latte with your phone instead of pulling out cash or credit card. But there's something else in play. Mobile payments, if you look at how they've been deployed in developing economies have been really economic drivers for the cash-light and financially inclusive economies that they create. But in more developed economies, with greater access to banks, what happens almost immediately with the introduction of mobile payments is a move to couponing.

So your phone is also your loyalty card. The app keeps track of how many times you visited that store, what you've purchased at Starbucks and the information is then used to generate offers, discounts and coupons that

keep you coming into Starbuck's store. It's these ease of couponing, redeeming rewards, and loyalty-like card features that are driving the acceptance of this, but also a really rich terrain for behavioral advertising.

MR. OLSEN: Tom.

MR. LENARD: I don’t see any rational that we've identified that has a separate privacy regime for telecom companies or cable companies. I think it's just kind of a function of the legacy regulatory system that's out of date, in terms of many of its characteristics, but I don't that necessarily implies that we should have a general privacy law.

MR. OLSEN: Anyone else want to weigh in here?

MR. HALPERT: The Internet Commerce Coalition includes both e-Commerce companies that are not ISPs; it includes advertising companies; it includes job search sites, and it includes ISPs. The consensus of the organization is that it does not make sense to have sectorial laws, and that includes not just ISPs who are telecomm and cable operators, but also the commerce companies that the regulatory system is out of date and ideally, if, for example, there is a code of conduct that's implemented in this area, it would be great if it superseded existing sectorial regulation because it doesn’t make sense to have two different overlays of

requirements that, in some cases, can conflict, and at the very least, can be confusing.

MS. PARSONS: Should there be an overarching, then, privacy law? If we remove the sectorial approach, do regulators and lawmakers need to step in?

MR. HALPERT: Well, there isn't much that regulators can do other than the FCC, I guess, acknowledging that it's not particularly productive for it to be very actively involved in privacy when the FTC is sort of the leading agency to be engaged in the issue. But in terms of whether a legislation should pass, obviously it depends on what that legislation says.

Right now, looking at Congress, it appears unlikely that Congress will move a baseline privacy law, but as with all proposals, there can be ways to improve the law, it's just that I'm not holding my breath for legislation to pass Congress that would supersede the existing sectoral communications laws. I think that that's probably a ways off.

MR. PICKER: Part of how you assess it has to be -- I'd ask you, though I don't expect an answer -- which is how do you feel about the scheme you're running right now?

So the scheme you're running right now is a scheme where what happens is someone makes a mistake and

it's not clear that the consumers have seen that mistake, have relied on that mistake, have engaged with that mistake. You label that a deceptive practice. You then ask for a consent decree. You then regulate them for 20 years. MySpace must be delighted to know they're going to be around for 20 years. That seemed optimistic, right. That's the scheme we're running. So is that a scheme you like?

MR. OLSEN: We do like that scheme. That scheme is necessary, but perhaps not sufficient.

MR. PICKER: Random and episodic.

MR. HALPERT: The question may be also whether baseline privacy legislation passes without any FTC regulatory authority, which seemed to be the discussion a couple of years ago. I think the Federal Trade Commission needs to think about whether that sort of modified version of Section V with a much clearer or overarching but more specific requirements is a good replacement for the FTC's existing authority in the area because I doubt that the resulting privacy legislation would give the FTC broad rulemaking authority over privacy in the end.

MS. CAMPBELL: But all with our enforcement authority.

MR. HALPERT: You certainly would have

enforcement authority, yeah.

MR. OLSEN: Chris, do you want to --

MR. HOOFNAGLE: Yeah. There is an interesting narrative here written by Ken Bamberger and Deidre Mulligan at Berkley, discussing the advantages of our episodic, FTC enforcement. They argue that the indeterminacy of FTC enforcement is causing companies to act more responsibly than they would if they had a clear, single law that would cause compliance only.

MR. PICKER: This is a vision that the FTC can occasionally shoot a company and that's a good thing?

MR. HOOFNAGLE: Well, this is actually what the Congress gave FTC. Congress was wise in its gift, if you will --

MR. PICKER: That's the question.

MR. HOOFNAGLE: You know, the FTC can't go out and levy huge fines against these companies. It can negotiate agreements that get worked out that deals with some of the due process concerns, but at the turn of the century and throughout the century, we've had problems with evolving marketplace problems. And it's very difficult to motivate Congress to pass a single law to deal with these different predations upon consumers.

MR. PICKER: That’s interesting because that goes back -- I mean, you were talking earlier about how

democracy acts in this space and you would think the democratic thing would be for Congress to do something. That's where democracy should take place, and not just at the FTC.

MR. OLSEN: Sid, I wanted to ask you this question as well, in terms of standards. I mean, you're in the tech innovation space and you're all about technological solutions to give consumers control and you're with a company that is competing on privacy in many respects.

Is it your view that competitive efforts to provide consumers with privacy are likely to prevail and are likely to be sufficient? Or do you think that additional measures might be necessary to address some of the issues that have been teed up today?

MR. STAMM: I wish I had an easy answer to that question. I think that's tough. I think that the people who know best how to optimize privacy -- the balance between privacy and functionality of things are the people making the things, the people innovating.

The people who best know how to compete for consumers' interest are the ones in that marketplace competing for it. To a certain extent, as far as online goes, you can go cross-sector. Like, browsers can do stuff to help people protect their privacy on websites,

but it gets a little fuzzy there because although we can share something that blocked all tracking, it makes the Web less attractive and less nice, and there's less you can do, and there's less innovation.

So there's no real easy tech solution to say yes, this is going to solve itself. And I can't predict the future. I wish I could. I really do. I'd be investing heavily right now. I think there's something to said about competition is affecting privacy in a positive way. Some companies are competing on privacy, but it’s not enough. I'd like to see it more. Take it as you will. That's coming from Mozilla. I think technology cross-sector can help out a bit, but I don't know what we need.

MR. OLSEN: Well, let me ask you a different question. In your view, is there a stronger incentive by companies to engage in additional and integrated data collection or is there a stronger incentive for companies to compete on privacy?

Just your outlook on the marketplace today, where is the incentive structure and where do you see companies moving?

MR. STAMM: So those are apples and oranges, right. Companies are going to compete on privacy if they want to compete on privacy and companies are going to

collect data is they want to use the data.

MR. OLSEN: Quantify it then. Do you see more apples than oranges?

(Laughter.)

MR. OLSEN: Apples being companies wanting to innovate by collecting more consumer data.

MR. STAMM: Okay. I was going to say I see a lot of Mac Books in here. I can't quantify it. I don't know. I'm sorry.

MR. OLSEN: Okay. Real quick, Jim.

MR. HALPERT: I would say that companies that have strong relationships with consumers, first-party relationships, balance those interests very carefully and do privacy reviews before deciding whether to move forward with glomerations of data from multiple channels from which they might receive it.

So the first-party relationship does very much come into play, and how consumers are going to respond is a very important factor. There are many more marketing ideas that are rejected than are accepted. They're rejected, very often, for privacy reasons.

MR. HOOFNAGLE: If may sharpen your point, you often see better behavior from first-parties, but you frequently see the best behavior from parties that you actually pay.

The company, whose business model is free, are often hiding privacy as part of the price. If you look at let's say the difference between Apple and Google, they are a very different incentive structure for a collection of information and treatment of consumers.

We recently had a speaker at Berkley that discussed Google, from the industry, and he said Google wants the internet to be free so it can sell advertising. Which I thought was actually a pretty profound point. One of the points I've made in a recent article with Jan Whittington is we need to think about paying for more items, more services, et cetera, because if we were actually paying these companies, there would be a better incentive alignment. And that might be a way of avoiding regulation and having the market shape these problems in a way that is more privacy friendly.

MS. PARSONS: Sid, did you want to weigh on this anymore? Then we're going to final --

MR. STAMM: Yeah. I was just going to jump in again. I'm an engineer and I was going to answer your question like an engineer and say 20 percent to 40 percent or something like that. So that's why I can't quantify it.

I think, what's been said, since I admitted lack of knowledge there, was that trust does play into

this a lot. So companies can compete on trust. Privacy and security are inputs into how much consumers will trust the companies they're interacting with. If you have consumers who aren't going to leave you for any reason, you don’t need the trust as much as you do if you're competing. I think a lot of companies are competing on trust now, and privacy is part of that. I don’t know how much, but I'd like to see it more.

MS. PARSONS: Okay. Well, we are running out of time. So I'm going to give each of you an opportunity, 30 seconds to a minute, to wrap up your thoughts on this very broad topic. We'll just go straight down the line. Chris?

MR. HOOFNAGLE: I've been here the whole day and one of the things that struck me was how different individual's assumptions are about the marketplace and how things work. On one hand, we're seeing some arguments that are very rational actor-based, with the idea that we're all autonomous individuals just behaving in the market and "that what appears" is good versus people who want to look more at the environment and study how the environment shapes our understanding of possibilities and how the environment shapes our decisions.

I was at the zoo the other day with my 2-year-

old and we saw Santa Claus. I said well, maybe we'll go talk to Santa Claus. Santa Claus asked him, "What do you want for Christmas?" And my son said, "Grilled cheese."

(Laughter.)

MR. HALPERT: I can agree with that.

MR. HOOFNAGLE: We were actually in a restaurant. So I think context told him to ask for that.

MR. HALPERT: Sounds like a good deal for mom and dad.

MR. OLSEN: That's my reaction too.

MR. HOOFNAGLE: My point is that in thinking about consumers and their expectations, we don't know about all the possibilities. And there are very privacy protective alternative business models to this massive collection of data by third parties, but we're treating the current path as the only one.

When I hear about all the riches at the end of the OBA path, I'm reminded of the miracle of instant credit and all the promises and hope that were unsubstantiated there.

MR. PICKER: I agree. It's been a very interesting day and to see how different people approach things. So we seemed to have spent most of the day on the failures of the marketplace, which is not my average day's take. So that's been interesting.

I think it's important to focus on potential harms. I really think it's important not to lose the eye on all the benefits that this system has generated for us and I don't think we should treat the government as being free. It never is.

MS. CAMPBELL: I'd close with a point on the intersect between trust and privacy. So I think that giving users back control over their own information and pressing for things such as greater user control over it, the right to be forgotten on the internet, the right to anonymous access, and more generally, embedding accepted FIPP principles into emerging technologies. And picking up on what Chris said, perhaps options to pay with money or pay with your personal information.

Doing those things may actually serve to increase competition, which could, in turn, lead to greater innovation.

MR. HALPERT: I'd conclude by saying that the overall purpose of this workshop was to look at whether the FTC's notice and choice and Fair Information Practices model that was developed through the staff draft and then the report that was issued in March should be changed due to this model of -- I think comprehensive data collection is the wrong word. This definition should not -- this whole topic should not be

comprehensive data collection. It should be a lot of data collections. I think probably really what this workshop is talking about.

I think, overall, my take away from this is that there should be certain uses of information that are collected in this manner that should be prohibited. And that it's important for businesses that engage in collecting a lot of information to look carefully at the transparency that they provide to consumers and that their overall data practices, you know, how long they're keeping data and what sort of notice they're providing. Are they providing consumer choice? Those are the sorts of take aways that I think we should draw from this informative and interesting day.

I agree with Chris that a lot of the speakers were approaching this from very different points of view. All well expressed. But I think in terms of an action item, I think we should continue education and to look at barring certain uses if they're not adequately barred by self-regulatory frameworks today. So I'll just conclude with that.

MS. COOPER: Two points. The first is that I think -- and just reflecting on everything that I heard today -- is that there's not really a privacy framework that I know of or any particular regime in any sector

that allows for unjustified, unexplained, limitless collection and indefinite retention.

I do think there is something to be said for the fact that, historically, that framing has been accepted as a risk and a reason to try and build in some limits. So I think that's an acceptable framing for this conversation.

The second point is that -- getting into the topic that was raised a lot, earlier today, which was about technology neutrality -- I think we heard a lot this morning about deep packet inspection, DPI, and we didn’t hear very much at all about content delivery networks or anyone who operates a domain name server or anyone who operates a Web proxy.

There are all kinds of technologies that can be used for essentially very similar purposes and not just on a sector-by-sector basis, but even what can a network operator use. What can an operating system vendor use? What can a device maker use to do data collection? I really think we should stay away from trying to evaluate these practices on the basis on which technology is being used, in part, because I think DPI does have bad name now for various reasons. And one thing that encourages is companies to call what they're doing something else so that it doesn’t attract the attention that DPI would

attract. I'm not saying that's happening, but it certainly is something that does happen. So think extreme caution necessary on trying to be technology-specific.

MR. HALPERT: Don’t beat a dead horse is the other rule.

MR. LENARD: I would like to just return briefly to the competition issue, which is obviously important to the FTC and I don't think it's been discussed enough today. If you're looking at somehow applying special rules to a subset of entities, however its defined, but who are presumably all major players in the internet ecosystem, I don’t think you want to make it more difficult or perhaps, even impossible for those entities to use information in order to innovate and compete, and particularly, compete in areas like online advertising. It seems to me you want all of these companies to be competing with each other.

MR. STAMM: This is dangerous giving the computer scientist the last word, and third to last word. This has been a really, interesting day for me. I've learned a lot. I learn a lot every time I attend one of these. What I'm taking away from it is that the first problem we should solve is this gap between what people think is going online and what’s actually happening

because we need to get consumers back into the picture and connected with what's going on so that they can voice their concerns. After all, that's what we need to deal with, right, their concerns.

In fact, there is no Web without them. There's nothing, except a bunch of companies trying to sell to each other. We need those individuals to participate. We need their trust for innovation and for accurate everything, online.

There's no silver bullet yet to make this happen. We need to work on that. Ultimately, like Lisa said, the first step is giving consumers back control over their data. So the internet is complex. This comprehensive data collection problem is not trivial, not in the least, and that's why we're spending so much time on this. And that's why we're here today. We need more data to figure it out.

MR. OLSEN: Thanks, Sid. I want to thank everyone. I hope that people did not approach this third panel with the expectation that we were going to resolve, by consensus, the problems of either comprehensive data collection or a lot of data collection. But hopefully we did explore some of the issues in enough detail. I do expect that we will be eliciting comments.

One issue we did not get to, and there may be

some consensus on this, is the issue of prohibited uses. There seems to be some consensus that there are some uses that ought to be prohibited. We didn't get a chance to really examine what those are. Hopefully that we can get via comments.

So I want to thank everybody on the panel. I want to turn it over to Maneesha Mithal, the associate director of the privacy division, who is going to give some brief closing remarks.

CLOSING REMARKS

MS. MITHAL: Okay. So since I'm the optimist in the group, I thought I'd close by kind of eliciting some of the consensus points that I heard today, but before I do that, I just wanted to thank everybody in the audience for being with us today, for sticking it out to the last panel, those on the webcast who have been watching all day. I especially wanted to thank all of our panelists who took time from their busy schedules to engage in the discussions, roll up their sleeves. I really thought the discussions have been really, really lively. I especially think their contributions are important because we did invite a lot of the companies to speak today who have the capability to engage in online comprehensive data collection, and many of them declined to participate.

But we do want to hear from you, so we are going to keep the record open for this workshop and we're going to accept written comments. So you can go to our website for the workshop, which is at ftc.gov, and find instructions on how to submit written comments. So I would encourage those of you who didn’t attend, those panelists, those who are watching on the webcast to submit comments.

Okay. So what do I see as the areas of

consensus that have emerged today? Let me just point to five of them.

First, I think that what we talked here, comprehensive data collection versus a lot of data collection, I think we all agree that there are lots of business models that are out there that can permit an entity to get a pretty comprehensive window into consumers' browsing behavior.

Now, there was some disagreement over kind of how comprehensive that data collection is. I think we heard this morning from Ashkan that Google, for example, can get 88 percent of your browsing behavior. Another panelist emphasized that consumers are accessing the internet through all sorts of different channels at work, at home, through their mobile devices. So you don't necessarily have one entity with a comprehensive picture of people's browsing behavior, but you can get pretty comprehensive.

Second area of consensus is that there are numerous benefits of tracking. We heard a lot today. We heard about the Google anticipating flu trends. We heard about cities using traffic flow data to figure out where to put traffic lights and that sort of thing. We heard that people can get more accurate performance information, and of course, we heard about the free

content that advertising fuels.

Third consensus point is, along with the benefits, there are also risks to comprehensive tracking. And this is where I'm maybe going out on a limb by saying there is consensus. I heard from Howard Beales that not only are there potential -- that financial and physical harms are not necessarily the only harms that we might want to consider when looking at this area. There's also reputational harm. And we heard the Designer Wear example and we heard the porn hotel example and we heard a lot of other examples of reputational harm. I think where the consensus tends to break down is that there seems to be disagreement over whether collection itself is a harm.

I think we've heard from some people, Chris Hoofnagle talked about the space to be away from surveillance. We heard earlier today about the concept of intellectual privacy and the idea that I should be able to ask a question on the internet or to my friends without that question being broadcast all over town. So there was some, I'd say, lack of consensus on the issue of whether collection itself is a harm.

Fourth area of consensus is the need for tech neutrality. We can't be picking winners and losers in this space.

And then finally, I think especially in this last panel we heard a lot about the fact that competition on privacy should be a goal. Maybe we're not there yet, but that's something that we should be striving for.

In closing, I think the most important part of what I wanted to do in my closing remarks is thank the FTC staff who have made this workshop such a success. I want to start with David Lincicum, who is sitting in the corner there, who spearheaded this whole workshop, along with Peder Magee, Katie Race-Brin, Kandi Parsons, Paul Ohm, Chris Olsen, Doug Smith, Cheryl Thomas.

Also thanks to Samantha Constat, T.J. Peeler, Wayne Abramovich, our wonderful paralegals and our media team for making sure that all the logistics for today worked out. Thank you again for coming.

(Applause.)

(Whereupon, at 5:05 p.m., the workshop was concluded.)

* * * * *

CERTIFICATE OF NOTARY PUBLIC

I, GERVEL A. WATTS, the officer before whom the foregoing meeting was taken, do hereby certify that the testimony that appears in the foregoing pages was recorded by me and thereafter reduced to typewriting under my direction; that said meeting is a true record of the proceedings.

GERVEL A. WATTS
Notary Public in and for the
District of Columbia

My Commission expires: January 31, 2014