>> ELLA KRAINSKY: Welcome back, everyone. We'll begin our final panel, Mobile Privacy Disclosures, with a presentation about downloading apps with Manas Mohapatra and Andrew Schlossberg from the Mobile Technology Unit of FTC's Division of Financial Practices.

>> MANAS MOHAPATRA: Good afternoon, everyone. Before we get to our last panel of the day, we wanted to start off the conversation by presenting some information about the process of downloading an app. Our next panel is gonna discuss the opportunities for privacy disclosures in the mobile space. But prior to delving into that topic, we want to make sure that everyone here has an understanding of some aspects of what a typical user sees when they download an app. We're gonna walk through the app-download process on both the Apple and Android platforms, and we hope that you'll keep some of the upcoming screen shots in mind during the next panel. We're gonna start by walking through the app-download process on an Apple device. Here, we start with a screen shot of an iPhone home screen. That's the first screen that you would see when you turn on your iPhone or iTouch. For the purposes of this presentation, let's assume you want to download an app that's useful for space exploration and stargazing. The first thing that you'd need to do would be to access the App Store, which can be reached by clicking on the blue App Store button, seen here circled in red. This would take you to the App Store home screen, where you could search for different stargazing apps and click on the app that appeals to you in the results. Now, let's say that the stargazing app that you're most interested in is called FakeApp. When you click on the app from the search results, you'll be taken to a description of the app. And what you see here is the description page for FakeApp. From here, you could install the app by clicking on the blue "install" button, or you could scroll down to find the description and screen shots of the app, ratings other users have left, the date of the last update of the app, and sometimes a link to the app license agreement. If you scroll down from the first screen of the app description, you can find more information about the company that created the app, including the address of the company's Website, which is not hyperlinked, along with a button called "app support." If you click on the "app support" button, you'll likely be taken to a Webpage on the app developer's Website that contains more information about the app, likely in an FAQ form. If you decide that you do want to install FakeApp, you can scroll back up to the top of the description page and click the "install"

button. After you click "install" and enter your password, this pop-up box would come up, and you'd have to click "okay" for the app to download. Now, after the app is completely downloaded to your phone, the icon for FakeApp would appear on your iPhone's home screen. To use the app you've downloaded, you just click on the app's icon from the home screen. Now, what you see here is what you'd see after clicking on the FakeApp icon and launching it. And one of the features of FakeApp is to find your location for purposes of determining what constellations are nearby, as well as to show you your location in relation to space-related events, like shuttle launches. Once you attempt to use one of the app's features that actually requires the use of location information, you'll see a pop-up button like the one seen here on the left side of the screen. You can allow FakeApp to use your location by clicking "okay." Now, any application that wants to use your current location would ask you for permission with a similar prompt. If you want to see a list of all the applications installed on your phone that do use location services, you can go to the iPhone's settings and look for "location services." From there, you could also turn location services on or off globally by using the setting that's at the top of this page on the right-hand side, or you could turn location on or off on an app-by-app basis.

>> ANDREW SCHLOSSBERG: So, let's now look at the Android platform. From the Android home screen, look for the preinstalled Play Store, circled in red on the slide. You'll be taken to the Google Play Store and would need to type in the search term "FakeApp" at the top of the next screen. After finding FakeApp from the search results, you click on it to arrive at this screen -- the app description. You can click the blue "install" button right away, but if you want to scroll down, you will see the app's number of downloads, ratings and reviews, date of its last update, its size, app screen shots, and a description of what FakeApp does. If you scroll down a little further, you'll get to this screen. You can visit the developer Webpage, which will open a mobile browser if you click on the link, or you can send an e-mail directly to the developer if you have any questions. This is unlike the iPhone, which does not list an e-mail address for the developer and does not hyperlink to the developer's Webpage. In addition, you can also see Google suggestions for similar apps that users have downloaded. After reviewing the FakeApp description and clicking on the blue "install" button, you arrive at this permission screen. Permissions essentially let the user know pre-download what information the app will access while running. This feature is unique to Android devices. You can click "accept and download" without looking at any of these permissions, but if

you'd like, you can read them before accepting. Here is one example of a permission. If you click on "your location," seen at the bottom of the previous slide, you are taken to this screen, which further explains what it means for FakeApp to access location and what happens if most apps obtain it somehow. Note that you can't opt out of any particular one of these permissions, but you can learn what the app can access before the app actually starts to download. Also, the permission disclosure is just a notice, as it does not tell the user why the app wants the information or what it does with it. After reading or not reading through the permissions, you can now download FakeApp. After the app downloads, this screen pops up, and you are given the option of either opening the app or uninstalling the app. let's say you decide to open the app and not to uninstall it. Before you can access the app homepage, you must either accept or refuse the app end-user license agreement, the EULA. You have the ability to scroll through the entire agreement, or you can just click "accept" right away. If you click "refuse," you are taken back to the FakeApp open/uninstall screen, and the app does not run. Assuming you click "accept," you are now taken to the FakeApp homepage, seen here. From this page, you can access a number of functionalities related to stargazing and space exploration in this particular instance. Now, as Manas stated earlier, one of the features of the FakeApp is to use your location to stargaze, as well as to show your location in relation to shuttle launch schedules. For the Android platform, the app already has access to information through permissions, but you do have the ability to turn off location globally for the entire phone, seen here on the left side. Like the iPhone, you can turn location off globally, but unlike the iPhone, you cannot turn off location on an app-by-app basis. As a result, for Android, if you don't want FakeApp to access your location, you also wouldn't be able to use location for, say, the maps app or any other app on your device that uses location. So, that sums it up for the Apple and Google app-download process. Obviously, there are other platforms that we could have shown you, but since our time is limited, we wanted to take a look at the top two platforms. We hope this presentation will stimulate discussion about privacy disclosures on the panel to follow. Thank you very much. [Applause]

>> RYAN MEHM: All right. Thank you, Manas, and thank you, Andrew. Good afternoon. My name is Ryan Mehm, and I'm an attorney with the FTC's Division of Privacy and Identity Protection. I will be serving as the moderator for this panel, addressing mobile privacy disclosures. The purpose of this panel, as Commissioner Ohlhausen mentioned this morning in her opening

remarks, is to examine privacy disclosures on mobile devices and consider how they can be short, effective, and accessible to consumers on small screens. We also tend to explore what steps businesses in the mobile space can take to communicate with consumers in a clear and consistent way about their privacy practices. Today, you'll hear from six people who've spent a great deal of time thinking about and/or developing solutions about how to convey critical information about privacy to consumers on mobile devices, including what information is being collected, with whom is data being shared, and does an app collect or share location data. We are extremely fortunate to have with us here today Jim Brock of PrivacyChoice, Professor Lorrie Faith Cranor of Carnegie Mellon University, Pam Dixon of the World Privacy Forum, Sara Kloek of the Association for Competitive Technology, or ACT, Kevin Trilli of TRUSTe, and Ilana Westerman of Create with Context. In terms of the format for this panel, Ilana is going to kick things off with a foundational presentation covering research she has conducted about what consumers know about privacy and care about privacy, general principles she has developed that are intended to increase transparency and trust, and a new disclosure concept for mobile devices that she's in the process of testing. After Ilana, Sara, Jim, and Kevin will give brief presentations, and then we'll have a facilitated discussion exploring some of the issues raised in the presentations, as well as other issues. Before I turn the mike over to Ilana, I wanted to mention a few administrative details about questions. For those here in person, if you have a question you'd like to ask of the panelists, you can write it on one of the cards available in the registration area or from one of the staff here in the room. If you have a question, please write it on that card, raise your hand, and FTC staff will be moving around the room, collecting the cards and submitting them to me. If you're following on the Webcast and would like to submit a question, you can e-mail ftcdisclose@ftc.gov. Someone here is monitoring that e-mail address and will be reviewing questions submitted via e-mail and will ensure that those questions get passed on to me, as well. We likely won't be able to get to everyone's questions, but we'll do our best to incorporate as many as we can into the discussion. And now I will turn things over to Ilana. Thank you.

>> ILANA WESTERMAN: Thank you, Ryan. Okay. So, before I get started with the presentation, just a little bit of background on the Digital Trust Initiative. We are funded by a series of sponsors -- Yahoo!, AOL, the Future of Privacy Forum, Verizon, and Visa. But this is an unbiased, independent effort, and the results of the research and of the design are not something

that's directed by our sponsors. But we do want to thank them. [Laughter] And, also, just a little bit of background before I get started on some of our findings. As a design firm, before we even get started creating anything, any kind of pictures, any kind of drawings, the first thing we want to do is really deeply understand who we're creating them for, so we really want to understand the context of use. And, so, how we do that is we really go out and try to understand consumers. What are their behaviors? What are their expectations? What do they know? What do they care about? What don't they care about? And then based on that, what we do is we create a foundation -- a foundation that guides the design of guiding principles and best practices. So, once we have these two foundational pieces in place, then we can start innovating, and we start creating designs. But we're never right the first time, so it's an process of iterative test and design where we create, test, refine, create, test, refine. So, today, what I want to do is take you through a little bit of the context and the guiding principles piece, then spend the most part talking about the innovation piece and kind of where we're at with trying to create transparency and control of mobile devices. So, the first thing for the context piece, one of the things that we found in the research was that consumers' expectations are that maybe companies have access to their data and potentially. They have much lower expectations that companies are actually using or storing their data for any reason. And they happen to have a really low expectation that companies are sharing that data for any reason. So what happens is because consumers have such low expectations, they're not actually going out to check to see, "Oh, am I right? You know, is my data being shared." They don't expect it to be there, so why would they expect to have a control. But that doesn't necessarily mean they don't care. They really do care about transparency and choice. And it doesn't mean that they always want to act on it, but they want to feel that they know what's going on, and they want to feel that they have options. So, then we said, "Okay, well, people have expectations that aren't necessarily correct, but they really do care, so, you know, how do we solve for this." Well, the privacy policy is definitely one way to solve for this. They can go read about it. What we found in the research is consumers just really weren't going to read a privacy policy. I think this has been brought up in the past. And especially on mobile devices, what we found is they really didn't want to read them on the small screen. They would prefer if they were gonna read them to go to the Web. Now, with that said, when they saw privacy policies that were not designed well, felt they had to scroll left to right, up to down, loads of pinching, they felt that the company didn't care about them, so it could erode trust. So we're not saying that you shouldn't do well-designed privacy policies, but it's

probably not the vehicle that's gonna really make people aware at the end of the day. So, how did we found out what they care about? Well, one thing we did was a series of eye-tracking studies. And, again, consumers aren't going to privacy policies, but as part of the research, we asked them to go read privacy policies. And this one right here -- you see the red? That's a heat map. And what that red shows you is, you know, more consumers looked there or more consumers spent more time there. And it's about choice, so this is what they wanted to focus on on the page. Also, what we found is that consumers aren't going to check their expectations. What happens when their expectations are violated? And usually, this happens when something happens in their world, something they don't expect, or, more frequently, maybe they read something. So as part of this research activity, we have them go ahead and read a blog post about how some of their data was being used. And this was a common reaction that we heard...

>> FEMALE SPEAKER: I know I'm not part, so the only thing I can do is go onto the search engine and search images and stuff like that and, you know, just whatever, general stuff. But they wouldn't be telling me that they were tracking what I'm doing on Google. I wouldn't know that unless I read this article.

>> MALE SPEAKER: Mm-hmm.

>> FEMALE SPEAKER: Yeah, I use Google a lot to look up, like, images and stuff, 'cause I do a lot of crafts. And I don't really feel like I need to have people putting together data to change the environment with more relevant ads on the searching site. I can search on my own, yet they're, like, using my stuff and tracking it to put together some kind of thing for me. I didn't ask for that. So...yeah, I think that definitely people should be able to opt-out of that and be able to say...

>> ILANA WESTERMAN: When they have an expectation for how their data is being used, they feel like they've had a choice. So I'm gonna play this. Same article we had someone go read, and this is the opposite reaction.

>> MALE SPEAKER: It's not surprising. I think that the tradeoff from the start has been that for us to have access to these services where, like search, like Facebook, like mail, like all of these

things, there basically have been either free or very low cost. And I see what I would call the tradeoff, and I see that as a legitimate thing and, also, a fair deal, in my case, because a similar thing would be reading a newspaper, and, you know, you open it up, and there's an article, but there's also all these ads.

>> ILANA WESTERMAN: My own perspective, you know, if there's transparency and people have expectations, it's okay, but when they don't, it's not. So, what we find is design can really create that, and it can either create or erode trust. So if you're a trusted brand and you have transparency and control, what we find is, you have a stronger bond with your consumers. Likewise, if you're a trusted brand and you do something that maybe isn't transparent, doesn't provide control, consumers do give you the benefit of the doubt once, twice, a couple times, but eventually you start moving to an untrusted brand. But similarly, if you are an untrusted brand, you have the opportunity here to really move to a trusted brand by continually showing consumers that you have transparency and you have control, and so design can really help make that happen. So, moving forward from the context piece, getting into, okay, so now that we understand about consumers, what do we do? What's our foundation for design? So, these six guiding principles are what we use to really design, as you can see, the trust icon. And, so, first, we've talked about context, but the second one here is awareness, which is really important, especially when people aren't actively going out to seek information. How can we make them aware? But if they are going out to look for information, discoverability. Can they find it? Is it easy to find? And then if they find it, do they understand it? Do they comprehend it? Do they remember it? And finally, can they interact with it if they want to make changes? And lastly, what do they want to do, when do they want to do it, and how can we provide it to them in a way that doesn't get in the way, that supports them? So, we took those design principles, in combination with the research, and came up with 13 actions for how designers and developers create designs that build trust. So, I'm not gonna go through all of them. They are out on the Website if anybody wants to check them out. But I'm gonna go through the ones that are in bold. And the first one -- timing -- is something that we've talked a lot about here. And, so, when we first began the research, it really seemed like the Android platform would be really a great way to kind of provide consumers with what's gonna happen with their data, because right when you download, as we just saw, an app tells you. However, what we found is at that point in time, people weren't really ready to consume that

information. They were either trying to evaluate the app, not even sure if they were gonna keep it on their phone. They were just gonna see what is it like. Or they were just really excited about getting a new app, and they wanted to play with it, and then they weren't ready at that point in time to actually make a decision or read it. However, the app to the right there is a restaurant app, and when someone is looking at a menu and wanting to order something, they do pay attention. Of course they want their location to be used. I don't want to go to a restaurant in San Francisco if I'm in D.C., so I want to hit okay. So, I'm gonna play a video here of a consumer -- this was consistent across the whole study -- of reactions to we asked them to download apps on Android. And this is what happened.

>> FEMALE SPEAKER: Okay, and do you remember what they were asking permission for?

>> SAMANTHA: I don't read it. [Laughs] It's usually just -- I read it, like, the first couple apps I downloaded.

>> ILANA WESTERMAN: So, next, surface. And so this is something that is gonna be different for every app and different for every site. But it's the feeling consumers have if they have to take too many steps to find information, they may feel like it hasn't been surfaced. There's no golden rule here -- two steps, five steps, seven steps. It's just a feeling of the only way you understand it is through research to determine if your app really feels like you're surfacing the information. This was interesting here, too. Never would have expected it unless we actually tested it. But here at the bottom is a social network who allows you to turn on and off whether you want to share your data with other apps and services. But at the very bottom, if you read it, it says -- and I always have to look at it. Hang on. "All you information set to 'everyone' is available to friends, applications unless you turn off platform applications and networks." So, but there's no link there, and so there's no way to know where to go. So just a simple, simple thing like a link to help you go find where to make that can really help. Third thing is associating actions and outcomes. People really like this design constrict. It feels really easy to be able to turn things on and on. But you don't know what your benefits are, and you don't know what you're losing when you do this. You're just making a change. Which ties into this is really getting people a value proposition and letting them know kind of, you know, what they get and what they lose if they make a decision.

So, here to your left, it's telling you you're gonna get near-me services if you say "okay," but to the right is an example of a flashlight app that just doesn't tell you. It says, "I want to use your location." It doesn't give any information on why. So, now I'm gonna play a video of Dan kind of talking about this.

>> DAN: All right, so, even from what this is telling me, I still have no idea of how they're gonna use it. Like, let's say it says, "Hardware controls -- take pictures." What does that mean? Is it gonna take a picture of my screen and then send it to them? It says it can modify/delete SD card content. Does that mean it's gonna put stuff into my SD card? Is it gonna take stuff off? I mean, I don't know. This is extremely vague, and it's not like it's gonna tell me more if I ask for it, 'cause it's not given.

>> ILANA WESTERMAN: So, now we have kind of our design constructs. We have our guiding principles. We have the actions to take. And now really what we want to do is take those and let's see how can we move forward. How can we actually create this transparency? How can we create innovations? How can we make it so that consumers are aware, but we're not getting in the way? How can we make it so it's flexible for many different types of apps and services? So, this is just a concept. And I'm not saying -- We're in the middle of testing, and there's different some things that are working well with it and some things that aren't. But the process that we're going through of iterative test and design to refine we hope to get to something. So, I'm gonna go ahead and play the video here. And you'll see where the arrow's pointing in the upper-left-hand corner. If you go to a site that is gathering your personal information, there's an icon that appears. It bursts three times, and it goes to a slow glow. Then, if you're interested in knowing more about this site, you're able to pull down the shelf, and there is personal data being sent. And if it happens to be a site you care about, you can go look at it, and you can see what's being accessed. So, just to let you know, we prototyped this on the Android platform. It could be something that'd be on iOS and many other platforms, too. This is just an example to see if the concept even works. So, here, there's a consistent set of headers that would be consistent across all apps and Websites. And I'm not saying these are the right ones, but just an example. But then there's a lot of ability for each developer to program what makes the most sense for their app or service. So, they have two choices. Do you collect that information or not? If you don't, you'll see it's grayed out. And then if you do collect

the information, the app developer has two choices -- whether they're gonna give control or not to the consumer. So, let's say for location for this particular app, you really have to know location for it to work. You would not have the option to opt-out. But let's say you could of Web history and bookmarks. Finally, underneath each of these areas, it would actually give the value proposition and allow the developer to write in why it needs that information and even link to get more if the person wanted it. So, where are we with this? Well, our first concern was are people even gonna notice this icon exists? Are they gonna even see it? And so we were surprised and happily surprised that more people saw it in our first iteration than we thought. So we still think it might be a good direction to take. But this might not be the only solution. There may be many other innovations that might solve this. One thing we're doing quite with this is motivation. We heard from consumers that they don't really care about certain sites, and they care more about others. So their ability to go in and make changes to things they care about and not get in the way with something that was very positive. But we are still having some issues with discoverability and comprehension. And so here I'm gonna show you how we found out that people were aware. We asked them to spend five minutes just browsing. They had no idea what the study was about. And this is an eye-tracking study, and so what happens is it shows your eyes, and the red dot gets bigger the longer you look at something. So you'll see she's reading about Johnny Depp. This is something she wanted to read about it. [Laughter] And Ellen DeGeneres. I guess it was a good show. You saw, she went up and looked. Now, whether someone looks and whether someone remembers is different? So, after that five minutes, we gave them a blank piece of paper, and we asked them to draw what they saw on the screen. And a surprising number of people actually decided there was something up there flashing, so they had noticed it. However, our first attempt wasn't the best at awareness. Our first attempt, we call it the "glow only." We didn't really want to get in the way of the consumer. We didn't want to be irritating, to be flashing in their eyes. So we just had this soft glow in the upper left. We had pretty low awareness with this round of testing. So, second round of testing, we had this flash, this burst. And we were concerned that would be irritating, but it would only flash three times. And consumers said no, that's fine. But we still did not get the awareness that we want. So now we're looking into other techniques, like vibration, like different colors, and other ways to kind of gain awareness. Also, with comprehension, what does the icon convey? The goal really here is to have it convey my personal data and transmission. And, so, some of our icons are doing quite well on conveying transmission and other personal data,

but we really aren't getting good both together, so we had more work to be done to actually create an icon that conveys it properly. And finally, this is the area we're most concerned about, which is attention and retention. So, after people become aware that hey, this is available and that, you know, my personal data is being accessed and I could go in and change it, we gave them 30 more minutes to surf. And after that, we asked them which sites that you went to were tracking your information. And people did not tie the icon to the sites, so while they recognized it was there and it was kind of ambient in the background, we don't have enough of a link between it yet and the actual different sites and services. So, our next concept we're looking at is bringing it down from the top shelf right there into the bar for a browser, where you would actually see it next to the URL. And this will go into testing in the next month or so, so I don't know how it will do. So, just in closing, I'm required to put this up for all of you, but it is an independent effort, and we do really want to thank our sponsors -- Yahoo!, AOL, Future of Privacy Forum, Visa, and Verizon -- for supporting it. But this is an unbiased circuit. How can we create innovation in this space, not just what's wrong, but how we can actually move forward? [Applause]

>> RYAN MEHM: Thank you, Ilana. Before we have presentations from Sarah, Jim, and Kevin, I just wanted to ask a few questions based on Ilana's presentation. And the first is for Professor Cranor. And it's you recently studied the permissions models on Android smartphones, so I have a two-part question for you. Number one, what did research reveal? And, number two, what are your thoughts on Android's permission model compared to Apple's model?

>> LORRIE FAITH CRANOR: Yeah, we did some work at Carnegie Mellon, interviewing people about the app permissions. My student Patrick Kelly did this work. We found was that for the most part, people had very little understanding of the Android permissions. They didn't understand how the Android market worked. They had a lot of faith that somebody was protecting them from bad apps somehow in the App Store and that they had all of these permissions options on the screen that were kind of gobbledygook for them. We actually went through them one at a time and asked them to, you know, explain what they thought each of these permissions meant, and they had very little idea. And even things like location, which you might think is relatively straightforward compared with some of the other permissions, people still weren't entirely sure where the phone was getting their location, at what granularity, what it was doing with it, or why. So really not a

whole lot of understanding. We didn't look specifically at the Apple store, so, you know, a lot of this is kind of speculation from our experience. But, you know, the difference that you have here is that, you know, on Android, you are actually presenting this whole list of permissions which you don't have in the Apple experience. But on the other hand, you do have some fine-grain control over location on the Apple side which you don't have on the Android side. And I think that fine-grain control is something which is a good thing, but it would be good to have it not just for location.

>> RYAN MEHM: Thank you. Let me ask Pam a question here. One of the things that Ilana's research has elucidated and that Jen King hit on earlier today is the relevance of the timing of a disclosure, and by that I mean the notion that a disclosure might have little meaning for a consumer in one context, yet that same exact disclosure may be highly relevant if made at another point in time. So, again, a two-part question. Do you agree with this notion of timing, and what are some other potential methods that businesses can use beyond a privacy policy to provide consumers with appropriately timed notice about their privacy practices?

>> PAM DIXON: Thank you. Well, I'm actually looking at these 13 design things. I want to get to your question. I like the idea of timing. I think timing is an issue that's very important in privacy. And it's a front-end design issue. I don't want to focus just on design. I like your principles a lot. I think they're really interesting. I'd actually add a few for privacy. But timing -- I think that there's a design issue of timing. I like the idea of something popping up when it's necessary or when there's about to be a potential issue where a consumer needs to take a pathway, yes or no, opt-in or opt-out, or even being told that they're not being offered the option. [Laughs] So I think that these are all very good things, and I think timing is everything. I would say this, though. In looking at the 13 design principles, you know, when I think about the 2000 report, you know, they used, of course, different words. Some of the things I came up with is is the notice sufficient? Obviously, is it prominent? And when I think of sufficient, I think of in the 2000 report, they said something interesting. They said, "Don't be coy." I really agree with that. Don't be coy. So sometimes improving notice just means be honest. Communicate what you're really intending to or your attorneys have told you to. And I think that that makes a big difference. Is it prominent? I think that this is something that's overlooked tremendously. So, we heard a little bit

in earlier panels about cross media. I think this is enormously important. Okay, so, I do believe in privacy policies. They have an important function. They need to be there, and disclosures need to be in a privacy policy. But why not also put disclosures in an app that people can download that's associated with the ad? I'll talk more about this in the Q&A period. Why not have disclosures that you can e-mail as reminders once a month to your favorite customers that are signed up in some kind of rewards program? There's no reason not to use every medium that's available to you. If you have a Facebook page, which I think every brand does now, or Twitter stream, why not place information there, as well? I say be robust and be creative with that robustness.

>> RYAN MEHM: Do you want to respond, Ilana? Ilana, do you want to respond to anything that Pam has raised?

>> ILANA WESTERMAN: Sure. I think the key thing is if we're trying to create the transparency, we have to put it in a place where people are actually gonna consume it. So just 'cause we put it somewhere doesn't mean that they're gonna actually look at it. So I think that's where timing comes into place and placement comes into place. But I definitely agree with you, kind of our guiding principles around making sure we're making people aware, making sure people comprehend and remember. So the six kind of guiding, foundational principles is where we're going towards. But I think the key thing is we can't control consumers and what they want to pay attention to, so as much as possible telling them when they can and giving them easy access.

>> PAM DIXON: Yeah, I think that's a really good point, and I agree with it completely. I also think that's incredibly important to provide a more permanent place of notice so that a consumer can have stumbled upon a fact, and they can find a notice after the fact if there's a problem. It may be a CMU story, or maybe they've heard a rumor. It's all very helpful to have something permanent that they can also find. So I think timing is important when you're installing and working with a product the first few times. I think what's interesting about your research and something that our research is also showing is that after a notice is read the first time, it's just toast. You can just put an expiration date on it and call it done. So we're really interested in seeing how other methods like e-mails and, you know, reminders are useful.

>> RYAN MEHM: Let me go back to Professor Cranor. You've done research on icons before. Based on that, what challenges exist regarding consumer awareness and understanding of the trust icon that Ilana and Create with Context has proposed.

>> LORRIE FAITH CRANOR: Right. So, we did a study on the advertising-options icon, which is now on a large fraction of ads that we see online, and we put ads in front of about 1,500 people which had this icon. And the vast majority of them didn't recognize having ever seen it before, although surely they had. We also probed them to try to see what they understood about it and whether they would be willing to click on it and to actually interact with their ad choices. And what we found is that a lot of them really had no idea what it meant or they had some ideas of what they thought it meant that were actually contrary to its actual meaning and counterproductive. So, you know, the idea is that you should click on it if you want to opt-out or find out about your options. People thought if they clicked on it, they would get more ads, and so they were afraid to click on it. It was actually the opposite effect. So I think that this is really problematic. We actually tested it with the various tag lines that have been proposed for it, as well as some others, and the ad-choices tag line actually didn't help. It probably hurt things, which was really problematic, as well. We've done some other testing with other icons, including some which I think are, you know, reasonably good icons, but privacy is not a concept that lends itself to little pictograms very well. And so even very well-designed icons -- they're not intuitive to people. And so I think the concepts that Ilana is talking about are really fantastic, but I am skeptical that will stand alone. I think that as part of a larger campaign, whether it's actually some educational component to teach people about these things through various channels, there I think, you know, they stand a chance of actually being useful.

>> RYAN MEHM: All right, thanks. Let me give Ilana a chance to respond, and then we'll turn things over to Sara.

>> ILANA WESTERMAN: Thank you. So, the advertising -- we haven't done any testing on that, so I really can't comment too much on that. But I can't imagine that that's a much more difficult space than what we're trying to do, because, first of all, you get attention on the ad, and we know that that's not 100% attention there. And then after you get attention on the ad, then you have to get

attention on the icons. So that's a huge challenge, so whoever's working on that, good luck. [Laughs] But yeah, we were concerned with the icon, as well, and I don't think it's necessarily the only answer. This is an innovation process, and it's an iterative test and design process. We actually were really kind of pleased how many people did identify the icon as being maybe human or maybe transmission. We thought we were gonna have to go through many more rounds of revision to get there. We were also really pleased, you know, that people kind of got a sense that it might be transmitting something. But I don't think it's gonna be the only way, and the only way we're gonna find out is to really test and continue to refine. But with that said, having done lots and lots of icon work and design work, I definitely think we can create things in that size to communicate things to people. So I don't think that's an undoable thing. It's just a little bit hard. [Laughs]

>> RYAN MEHM: So, next up is Sara Kloek of ACT. Sara will address disclosure issues and challenges from the app-developer vantage point, as well as the mobile badge developed by Moms with Apps, an affiliate groups of ACT. This badge has been designed to be featured on app-developer Websites and in app marketplaces in order to provide parents with information about kids' apps. And it looks like there was a bit of a color issue, unless my eyesight has gone bad.

>> SARA KLOEK: Uh-oh.

>> RYAN MEHM: But I think we're trying to find a tech person.

>> SARA KLOEK: Color issue. [Laughter]

>> RYAN MEHM: Thank you, Morgan. [Laughs]

>> SARA KLOEK: I'm gonna set, and I appreciate efficiency, so I'm gonna time myself and make sure I stay within the time limits. My name is Sara Kloek, and I am the director of outreach of ACT. We are the trade association that represents all of those mobile-app developers around the world. Today, I get to do the best part of my job, which makes it the best job in the world. I get to brag about the cool stuff that our developers are doing, specifically focusing on mobile apps,

privacy, and kids and an innovative privacy solution that they came up with. So, again, best part of my job, bragging about what they do. They make really cool technology. They're changing the way that we work, changing the way that we play, and changing that we interact with people, and I hope that they get to continue to do just that. They're moms and dads and grandmas and granpas, and they're making those apps that you use every day. One of the shining stars of the mobile-apps industry is Moms with Apps. This is an online, informal, collaborative group formed by four moms looking for new ways to cross-market their apps. It actually changed pretty quickly and has grown now to over 1,000 members on their online forum, talking every day, sometimes late into the night about best practices for mobile apps. They're talking about how best to increase sales in the App Store. What are some of the best languages to translate your app to so you can increase sales? And they do talk about privacy disclosures. ACT has worked with them since the beginning of 2011 on educating family-friendly developers on how best to include privacy in their mobile apps, incorporating COPPA, figuring out how to parental consent, and where to put your privacy policy when you have one and encouraging them to have privacy policies. So, when the FTC released their mobile apps for kids report, Moms with Apps was ready to react, and they got together over one weekend on the Internet, on their online forums, and started discussing what they can do. And over one weekend, some of the developers came up with a privacy-disclosure icon. They wanted to do what the FTC was encouraging them to do to disclose what information what they collect, if they collect anything, and what sort of stuff they do within their app. So, this is the first iteration, and there are other privacy icons, privacy disclosures. There's privacy certifications. This isn't a certification. There's other things out there. This is come up with from industry, from developers. Some of them are professional graphical designers, but not all of them are. They've been working on this for many months, discussing it in Webinars, discussing it in meetups, discussing it on their online forum and even on Facebook, presenting it to parents for feedback -- what they want, what they want to know when they're downloading apps. And this is one of the latest iterations that they've come up with. Obviously, they've changed the colors. They've changed what they've included. There are other iterations, and the developers are working together to figure out what they want to present to consumers and what consumers want to hear. Obviously, it's really hard to get over a thousand people to agree on something. We know that better than anyone here in D.C. And they are continuing to work and continuing to put it in their screen shots on the App Store. This is one of the earlier iterations? They put it on their Website. Here's another one. And this is

another one that is on the Website. Even within those three icons, you could see the changes. So, they have the icon, but it's clearly not done yet. There are a few things that people are wanting to know. The developers are wanting to know, parents are wanting to know, but one of the biggest ones is how do we know what to include in an icon. What do parents want to see? What does the FTC want to see us disclose? And you can't put 50 things in an icon. You can only put a set number of things that parents will see when the end users will see when they download. Where do we put this icon? Obviously, probably the most convenient place would be in the App Store, and the platforms are working on places where we can put this, and the developers are really happy about that. App developers -- how can we encourage them to adopt an icon like this? And the second question after this follows that -- how can we make this a positive icon instead of something like a scarlet letter. We want this to be something that would be adopted far and wide, not just on kids' apps, not just on games. We want it to be adopted far and wide. And then how do we get it so app customers know when they see this that, oh, good, the developer really cares about what my privacy is and trusts me and wants me to trust them. And we can discuss this more in the panel, but thank you, and I look forward to your questions and comments about the icon.

>> RYAN MEHM: Thank you. Thank you so much, Sara. [Applause] Next up is Jim Brock of PrivacyChoice, who will discuss PrivacyChoice's mobile PolicyMaker.

>> JIM BROCK: Thanks, Ryan. Go forward a couple slides here. So, PrivacyChoice's mission is to make privacy easier for people who publish, develop content and apps, and for people who use those apps. Part of what we do is we keep and curate a very large database of information about the privacy economy, which is to say companies that track users and collect data across sites. We make that available both for our own apps and for companies who want to license that data to make apps. In terms of mobile developers -- we've been focused on this for about a year now -- we developed a resource center for mobile-app developers to try to collect together different tools and resources, code, language, advice, excerpts from the App Store agreements, leading articles about techniques for anonymization -- things like that that we put into one resource center, including, as you can see from this, an entire set of privacy-policy language that we've made available under Creative Commons. To understand where we've gone, you have to understand how this was developed. As part of our core business, we've examined about 4,000 privacy policies and put

them into a taxonomy based on about 13 different categories and found that we could, for a very large percentage of those, put them into a taxonomy where there was one or four or five different, short statements you could make about location, about social networks, about how personal data may be collected, about advertising. This ended up culminating in the development of PolicyMaker, which is a wizard. It's about a 20-minute tool that a developer can go through. And the emphasis here is as much on the developers' education and understanding as it is on the end users' consumption of the privacy policy. 'Cause we know not a lot of end users take the time to read the privacy policy, but developers can do a better job of privacy if in the course of making that policy, they become educated about what it means. Do we retain IP addresses? How do we use cookies? What do we do with UDIDs? These kind of questions are things we try to handle in the tutorial and provide deeper information for the developer? This is what it looks like. And I picked this particular page from the wizard because it also showcases part of what we do on ad tracking, which is really one of the biggest challenges for a developer in providing privacy disclosure. 'Cause any number of third parties may be collecting data for analytics or advertising from within that app or their Web app. We collect all the information about those companies and allow the individual developer to simply pick the ones who are applicable, and we provide the disclosure. We provide the provide the proper links. We provide the summary of the company. We provide opt-outs in some cases when they are available on the Web app. So in that case, it becomes a more complete experience for users, because their choices are automatically embedded into the policy. Now, those choices are so limited. They still don't work very well for apps as opposed to Webpages. But it's a start, and we'll integrate with whatever tracking options may emerge from the industry. We also have a version of the wonderful icon. We put this at the beginning of our privacy-policy creation process, so you can't miss it, and it's very simple to set up and make selections and end up with the information. The last thing that didn't make the deck, because we just launched it today, is we've now launched an API for the privacy policy. You create one with PolicyMaker. What that really means is that your policy is available just as data. It's date that you can style to look however you want it to look within your app. It's data that anyone can look at. An App Store could look at the last date you revised your policy. You can take in an atomized sort of privacy disclosure where you want to present location disclosure here and social-network disclosure here in context. Those parts of the policy can be pulled out of the API and presented, but the policy remains a single, documented indication of the promises that the developer has made

to the end user. The API is a very exciting way to start stimulating people developing new, interesting privacy interfaces, and also allowing them to atomize their disclosure and say, "You know, location goes here. We're gonna provide that in context, but it's still part of my policy. I'm still responsible for it.

>> RYAN MEHM: Jim, thank you so much. [Applause] Next up is Kevin Trilli of TRUSTe, who will discuss creating a privacy policy and TRUSTe's short-notice privacy policy for mobile Websites and apps.

>> KEVIN TRILLI: Thanks, Ryan. Good afternoon, everybody. So, we just wanted to start with a quick showcase about some of the things that we've been thinking about. As you know, TRUSTe has been a certification company and a trusted third party for a long time and went private in 2008. And as such, at that point, we started looking at this more from a product and technology focus than we had done as a nonprofit historically. And the way we look at products is that we have, you know, traditional development, but we also have full-time user-experience professionals that look at this interface with consumers, 'cause it's very separate than the business side of the product. So, an example here I show is something we built several years back, which was really a tool that helped small businesses build policies, but really started to take a lot of flexibility with the way the output of that policy was created. What we're showing here is really a layer on top of the full policy. And this layer, based on what we did for research, really contains the key elements that a consumer may want, so different than a regulator, different than a class-action lawyer, but something that a consumer can look at and be actionable. So really trying to distill down the elements that a consumer can one look at and do something about that's practical. This concept is we refer to as "layered." We actually just updated the truste.com privacy policy last week and have a presentation of it there, if you'd like to see it sometime. One of the outputs really are the full policy, as we mentioned, this layered construct which really just sort of sits on top of the text, but also some machine-readable language that can be used in different ways. And what we're showing here is really a concept, the upper-left corner there, is a browser add-on that we built that really looks at these policies and does a little pop-up for three seconds and presents the states of those layered icons for the user so they can see it immediately, and then it just disappears very briefly. The concept there was how do you get a consumer to read a policy in three seconds? And that was

really the thought process that we put into that would really distill down what was contained in that output. The one on the bottom's a similar presentation that we had for European customers, but it's again presenting these key elements in ways that a consumer can look at them quickly and do something about. As we shifted to mobile, we looked at this in a similar fashion. There were things that were different, obviously, with the form factor and some of the disclosures, obviously, with location were different, but it's the same concept where it was really trying to get a user who decided to interact with us some information very quickly. The goal was not to have them spend a lot of time there to feel a warm and fuzzy trust feeling, that at least that the app developer was doing their best to present these elements in a trustful way. You know, and they can, of course, click down further to read more about it. But as we know, most consumers don't do that. When you start thinking more about it, you kind of combine these two concepts together with a layering concept and this mobile-app concept, and this is the current work that we have going on right now, which really just starts to combine the two and bring this information to consumers such that they can do something about it. I think the principles that we used when deciding what were these elements -- there are two really important ones, and I might cover these in the last slide. But first was really thinking about the things that are not obvious to a consumer that are hidden, that they can't see, that happen sort of after the data has been submitted. That's a very important concept, and really minimizing the number of disclosures you have. Consumers don't have time to read more than three things, frankly, maybe even just one in that blink moment of deciding that trust. So really, we thought through what are those absolute minimum things we can use to allow consumers to understand what's going on and then decide if they really want to learn more, go further into it. I did have that there. So, the other thing, I think, is also the annoyance factor. My previous life background with me, I had late-'90s work in the SSL padlock market for a long time, for five years, and really understood that concept of that blink moment of trust that consumers really relied on to submit their credit card for e-commerce. And I think the goal there was -- if you remember the early days, there were a lot of pop-up messages that would happen about certificates being invalid and all that good stuff. And that was corrected later, but really, this obtrusiveness or annoyance factor. If we go too far into disclosing too much, consumers will tune out even further in the other direction. So it's really finding that minimum set, and not just the timing, but the frequency of timing of the presentation of that, the length of which that appears, et cetera. That's all part of that kind of unique experience design that needs to come in when building these types of

disclosures. And, you know, I think that the key part is how do we know what's relevant to consumers? Final part there is from our research, consumers don't know. They are looking to experts. They are looking to government to tell them what's important and then rely on that in a trusted way. That could be the brand of the app. That could be trusted third-party brands. There's different mechanisms that have existed. But they really don't know from our research, and they're relying on someone to trust. And that's really the key part that I'll leave with. Thank you. [Applause]

>> RYAN MEHM: Great. Thank you. Thank you, Kevin. My first question is actually, Kevin, for you. In her presentation this morning, Jen King referred to the layered privacy notice and I think showed a TRUSTe slide. Jen noted that the layered notice makes it easier for consumers to find information, but doesn't guarantee consumers will read it. What are your thoughts, reactions to Jen's point? Well, you know, you can lead a horse to water, but you can't really, you know, take that next step. And I think the key is if they do go there, you know, make it so that it's written for them. Regular policies are not written for consumers. I mean, I think that's the first problem that layering is trying to solve is speaking a language that they can actually understand. I agree that, you know, in the layer, there's multiple things that need to exist, not just icons. There needs to be some text that explains them. There's also the concept of good and bad -- what's a good state versus a bad state? You know, I think, like, the security thing I was just talking about, there is a kind of common enemy with security where with privacy, it's contextual. It's built upon processes within a Website. There's so many sub-layers to it that consumers just can't get a good or bad measurement necessarily. So there's a lot of nuance that needs to be presented, and once they have the information, not just the choice but the tools they can use to control. And that could be technology stuff they download and use, or it could be interactions with the business. And I think the key to the layer is given that portal of things they can do that are actionable and over time, many years, they will become educated and trained on how to use that. It's not gonna happen initially.

>> RYAN MEHM: Let me ask a question of Jim. Jim, there is some real differences between your privacy policy generator and the one that Kevin just discussed that's developed by TRUSTe. For example, you both use different icons, and you both use different short disclosures. Can you

discuss some of the research and the testing you did to develop those notices and consumer awareness and understanding of what you developed?

>> JIM BROCK: Sure. Really, most of our efforts were direct focus group, traditional focus group stuff -- going to the shopping mall, actually showing it to people, an early build of it, and then making notes about what they did with it. What was interesting was it wasn't exactly what we predicted in terms of the areas of the policy that they would focus on. It could have been the icons we were using. Could have been lots of reasons. But one thing that a lot of folks focused in on was this disclosure that we'd all consider boilerplate, which is if there's a court order or if there's an extraordinary transaction, your personal data may be shared. We kind of de-brigaded that, and it turned out they were actually a lot more interested in that than we thought. The paradox here, the trick is that you have to serve consumers who both want that moment, as Kevin said, that instant-trust moment, but you've also got to serve the ones who really get into it and are really interested in privacy. They don't want to be handed off with too many icons and too much simplicity. They actually want to go kind of deep and really understand what's going on? And that I think is a challenge for icons, but I also feel like if there's a standard set of icons that emerge, we certainly would support that. The problem is, and I think, as you, Lorrie, eluded to, there's so many different permutations of policies, it's gonna be hard to have icons that are not in many cases cryptic to the user.

>> RYAN MEHM: Well, on the topic of icons -- and maybe this is a good question for Lorrie -- you know, the solutions devised by ACT, PrivacyChoice, and TRUSTe, you know, all incorporate different icons. How will consumers learn to recognize multiple, different icons, and should we strive for consistency?

>> LORRIE FAITH CRANOR: I think consistency would be a good thing. I mean, most of these are not just one icon. There's a whole set of icons to begin with. And if you have to learn three or four different sets of icons, I think that's really not gonna happen. So it'd be great if we could get some consistency in the icons, but also it would be great to have some consistency in the back-end metadata. I was really pleased to hear that this has a computer-readable representation which allows you to do so much more with it. But what's come up with one of them, and so we can have

apps and have the marketplace and have all of the phones be able to read that metadata and actually do stuff with it.

>> RYAN MEHM: Pam, question for you. Again, we saw three different proposed solutions here. How do they strike you from a notice and disclosure standpoint?

>> PAM DIXON: Thank you. I've had this feeling all day, and just if you'll bear with me, I'm gonna answer your question with a comment. So, really, I think what we've looked at today is all the different parts of an elephant, and we're all touching a different layer of it. So, we've seen folks talking about the design layer, or we've seen, even on this panel, talking about the policy layer. But what I'm gonna say is that there's a much bigger universe. And when you start talking about disclosures and privacy, the universe shifts a little bit. And I think we really need to talk about four things -- number one, back end, number two, front end, number three, we need to talk about online, and, number four, we need to talk about offline. We need to take into account all of these corners of the universe. So, for example, when I say front end, what I mean is that we've talked a lot about the design layer, the timing, the icon. We've talked about privacy policies, the front-end policy layer that consumers are going to read. This is great. I mean, it's terrific. But we also need to remember that those front-end layers are based on back-end layers. So, for example, a company may have a retention policy that allows data to be stored indefinitely. They may have a retention policy that sheds data almost instantly. They may have a use data that allows them to share data. These are very difficult concepts to convey in either icons or privacy policies. So I think we need to look at all of these and combine and join the front end with the back end and make sure there's a consistency of message and make sure that there's a persistency of message, too, so that it's timely, yet permanent. We need all of the elements. And consistency I think is a great word. I look at Ilana -- her phone, it's orange. Her Power DAC was orange. There's a consistency in that group's message. If only privacy policies were that way, we'd all be in great shape.

>> RYAN MEHM: That's a good segue to a question for you, Ilana. You mentioned that consumers don't want disclosures at the time they're downloading an app. What are some alternatives? And, in your opinion, is the only solution an icon?

>> ILANA WESTERMAN: So, definitely not the only solution, an icon, and the icon might not be the solution. I think the solution really is the goal, so it goes back to the design principles. What we want to do is we want to understand the context of use. We want to create awareness and attention. We want to make sure that people understand what we do, they comprehend it. We want to make sure they can find it if they're looking for it, like a privacy policy. We want to make sure it's easy to use. And, you know, we want to make sure we take into account motivation. What do people care about, and when do they care about not getting in the way? So I just think that there's a lot of different solutions. I just think that we're really early on right now in innovation space. And whether, you know, it's gonna end up being an icon or a centralized place -- maybe there's a lot of different places to explore. I just feel like we're a little bit too early on in the process to say, you know, we need a check box here or an icon there. We need that ability to continue to say, "Okay, we're gonna meet our goals, but we're not quite sure yet how they're gonna get to them."

>> RYAN MEHM: Thanks.

>> PAM DIXON: Can I respond to that? I agree with that. I think we're very early, and I think that it reminds me a lot of when AOL merged with Time Warner. And I got the press release on my desk, and I thought, "Oh, my heavens. This is a horrifying idea. It'll never work." And I didn't quite know why. I later figured out why. And right now, there's certain things I know that are very important for privacy and for consumers. I can't give you all the focus groups and tell you why, but I can tell you they're really important. I think icons are good. I think text is good. But I think having a lot of reminders, a lot of different platforms, and a lot of different ways and timings for consumers to access those messages, both online and off -- it's very important.

>> RYAN MEHM: In the interest of time, I actually want to move on to a different topic, 'cause we've got so much to cover in this panel. But the question is for you, Jim, so the timing is good. I want to move on next to the role of platforms and associations, so what are some concrete steps that platforms should adopt immediately to improve disclosures to consumers? And similarly, what can the platforms be doing now to make it easier for developers to make disclosures to consumers?

>> JIM BROCK: Sure. I think it's well-known that the California attorney general has come to an agreement with some of the major platform providers to start to embed privacy disclosure more closely into the App Store, which helps with part of the issue, right? It helps with the issue of if I want to know what the policy is before I download it, I can do that. And so that's obviously helpful. I know Mozilla's gone even further in a really good way, and they're actually pulling up four key policy terms into the actual experience. So you don't click over somewhere else. You actually see the four key policies, in their view, right on the top in the App Store. I think that's very helpful. It doesn't I think necessarily mean that we're training developers in a way that Ilana would to embed privacy disclosure and notices into the experience itself. And I don't know how much the platforms can help with that, except to point people to resources and do outreach and education. I think, frankly, and this gets back to Pam's comment, too, so much happens on the back end that affects privacy that is in many cases unrelated to the policy and what it says -- what information is retained and so forth. Just be requiring that they have a policy and to link it from the App Store is gonna have a massive effect on the attention paid to it by developers. So that is my answer. That's obviously the first big thing that could happen.

>> RYAN MEHM: This question is for Sara. What role can associations such as the App Developers Alliance or ACT play in educating consumers -- sorry, in educating developers on how to make disclosures to consumers?

>> SARA KLOEK: Sure. Well, I can't really talk about what anyone else is doing, but I can talk about what ACT has been doing. For the past year, we've been holding Webinars and meetups, and I've been traveling all over the U.S. and actually around the world, talking to developers about "Hey, here's some good options of where you can build a privacy policy. Here's some things you need to disclose. Contact me if you have questions. We've been hosting boot camps, because now developers are getting tired of all of these workshops and panels I guess, talking and talking at them. So we've held two boot camps so far where developers can go and actually produce a privacy policy and walk out with the answers that they need. They get the answers from the lawyers. And they want to be done with this. They know that privacy is an issue. They take it into consideration. They want to be done. They want to continue to innovate, making cool stuff, and changing our lives.

>> RYAN MEHM: Before we move on to the next topic, are there any other thoughts on the points that have been raised? Kevin, go ahead.

>> KEVIN TRILLI: I just had one question on the platform. So, I want to point out one good example. The Google Apps Marketplace, for business-to-business apps, did a great deployment with TRUSTe around integrating a privacy certification and policy disclosure like we showed inside the app marketplace that they have and their permission framework that's in the manifest reach-out that's submitted. So, this is the first example I saw of, really, the role of a platform. And Jim's points were exactly right. They control a lot of the power of the presentation layer to the consumer. And I thought Google did a great experience there of making that available for consumers -- in this case, business-to-business consumers -- for getting all that information up front.

>> RYAN MEHM: So, let's move on to different topic, which was a really big topic that's been alluded to on this panel and also others -- third-party data collection. Assuming third-party data collection is occurring via a mobile device, how should consumers be given notice that that is occurring and choice regarding whether they want to participate in such collection? Lorrie, why don't we start with you? And if others have thoughts, we'd love to hear them.

>> LORRIE FAITH CRANOR: So, we've been looking at third-party collections on the nonmobile platform. And I think we have a big enough problem just dealing with that. I think consumers still are taken by surprise by the fact that it's happening. They view it as kind of underhanded and behind their back and creepy. On the other hand, you know, when you can explain it to them, many consumers are okay with it once they understand it. So, I think there is definitely an issue of, "How do you actually communicate about it with consumers so they don't feel taken by surprise?" They also like to know they have choices, and we've found, though, that the type of choices consumers are presented with today are not meaningful to them. If you ask them, you know, "Do you want 24/7 Real Media, BlueKai, all these different ad companies they've never heard of to collect their information, they have no idea. They don't know who these companies are. They can't judge between them. And so I don't think we should take what we're doing on the nonmobile world

and try to move it onto the mobile world 'cause I predict lit work even worse than it's currently working. I think we do need to have ways, perhaps, with icons of showing people that the third-party data collection is taking place, but I also think we need to tell them more than the fact that it's taking place, but tell them a bit about what's going to happen to the data. And maybe what we need to do is to be able to come up with a small number of categories of things. So, you know, for example, you know, a third party collects your data. "We're gonna show you an ad, and then we're going to delete the data," versus, "We are going to collect it and keep it forever and do whatever we want with it." So, there could be these different categories. And then a consumer can decide among categories which are okay, which are not, and maybe even just set up their preferences on their phone and not have to deal with it on every Website, every app -- "Okay, I need to make a decision about this data collection."

>> RYAN MEHM: Jim, do you have anything you want to add on this?

>> JIM BROCK: Yeah, just two points. One is, I think one of the challenges -- and this is what we do with Privacyscore -- is separating more responsible data collectors from less responsible data collectors. And that even is another layer of challenge in the process, but it is knowable, and there are industry groups and certifications and TRUSTe has one. Others have them. And you can start to surface that in a compact way, and that's something we're doing a lot of. But on this point of third-party disclosure and also relating back to Pam's earlier point in the discussion about innovation, you look at what's happening in the E.U., you know, we're watching, you know, all these flowers bloom in terms of the different approaches Websites are taking to this very issue -- nonmobile -- right? -- nonmobile. But we're seeing the power of innovation when you have a little bit of a nudge to do it. And I think out of that, we'll look back 12 or 24 months and start to see more standards emerge and good practices emerge from that experiment.

>> RYAN MEHM: Let's move on to location tracking. And this question is for Pam. You have written and spoken extensively about the various forms of tracking that occurs on mobile devices, including tracking that occurs in the offline world through one's mobile device, as consumers move from brick-and-mortar store to brick-and-mortar store. What are some best practices that ought to be occurring to let consumers know that this is happening?

>> PAM DIXON: Yeah. Thanks. There's definitely a hierarchy of privacy priorities. On one end of the scale, you have display ads that are popping into your mobile phone that are just -- you know, you're searching for something, and up pops a little display ad. At the on the other hand is a retailer that is grabbing your unique Mac address from your smartphone or iPad and then is retaining that so they can track how often you come in their store. So, I think that we need to take into account that there is a hierarchy of this. And the best practice will depend on where something falls in that hierarchy. I really like the idea of -- Instead of thinking, "Okay, one privacy policy will fit all privacy priorities," I like thinking about some of the more intrusive privacy issues, like the snagging of a Mac address and thinking, "Okay, this is really akin to a negative option, and it needs extraordinary disclosure and a lot more attention and a lot more work." So, that would be my answer. The best practice is to look at what you're actually collecting, how long you're collecting it. Look at your backend policies. Make a determination on how you're using that data, how serious it is in terms of the privacy scale, and then start working on your front-end best practices -- the timing of the notice, the placement of the notice. Do you want to require consent or no? Do you want affirmative consent? Do you want a double opt-in? There might be cases where you want persistent reminders, as the 2000 report notes. So, I think that this is going to be highly contextual. But in general, I'd say that if you're going to snag a Mac address from someone, you had better have offline notice, online notice. You better be giving notice to the mobile phone. The more intrusive, the more robust and the more platforms you should be using.

>> RYAN MEHM: You had a couple of slides

>> PAM DIXON: Oh, I do. I do.

>> RYAN MEHM: Do you want to talk about them now?

>> PAM DIXON: Are they up? Yeah, that would be great 'cause it'll really exemplify that point. Okay, so this is just -- I don't want to pick on any particular companies. This is a really good illustration of -- If you're walking by a store that's grabbing your Mac address that your phone has, your smartphones or iPads, a store can just snag that from you. And they can snag it from you

before you're inside. So, this particular thing just shows that -- All they're doing -- They're not saying, "Oh, you know, Joe X-Y-Z shopped here, and we're going to You know, we'll gladly respond to any subpoenas for him, specifically." That's not what this is about. This is about -- Look, there were 12,000 people outside. Only 1,000 went inside. And you have X, Y, Z, repeat visitors from yesterday or even this quarter or more than a quarter. So, this company's retaining data for, we know, at least more than one quarter. This particular -- Next slide, please. This particular company is called -- Well, this is a report actually that we're getting ready to publish, very, very soon, like in days. There's a shop -- there's a lot of shops doing this, actually, but one of them uses Euclid Elements, which is a third-party company. It's named Philz Coffee, and it's in the Bay area. And this is their notice that they're doing this. They say, "We use Euclid analytics, an anonymous service for optimizing the shopping experience." So, a customer that walks in with a smartphone is going to read that notice and then be able to go to Euclid Elements. But in my analysis here, I think this is coy. It doesn't say that they're grabbing the Mac address, and it doesn't say, "If you want to opt out, go to this Website." Next slide, please. The truth is that if you do go to that Website, Euclid Elements, there's a permanent opt-out. The opt-out's good. And we have no problem with their opt-out. However, the thing is that that notice was only in one piece of paper, on, you know, one door in that physical location. That's really good, and it's an important first start because there's a bunch of companies that do the same thing and don't even give that much notice, and they don't allow an opt-out. But the thing is that this also needs to be showing up on the mobile phone when the Mac addressed is grabbed or, even better yet -- how about this? -- why not have a mobile app that says, "Okay, I'll download this mobile app and we'll give you a lot of love. You'll get a free coffee for downloading this app. And by the way, we're going to track your Mac address, but you know what? Here's the deal about it," and give people more information about it. Give them a robust privacy policy. An I just think an app might actually be a good solution here that gives people more information and more ability to make more choices. If you look at the privacy policy for this particular brand, this coffeeshop, the Website privacy policy doesn't even mention an opt-out, doesn't even mention that this is happening. So, there's to be consistency, and this is just a good example of why online and offline has now merged.

>> RYAN MEHM: So, Sara, Pam has suggested that there should be an app for that. What's your reaction?

>> SARA KLOEK: I'll let people know. I do have a quick comment on the use of Mace address and things like UDID and unique identifiers to the phone. That's not really private information. It's not tied to the person. It's tied to the device. So, we can argue about whether or not UDID and the Mac address should be something that is inherently tied to us, like our social security number. But I think that's for another panel and another day.

>> PAM DIXON: No, it's not. The Euclid Elements privacy policy is excellent because they're honest. They are not coy. They say clearly that that information can be correlated with your identity and subject is to subpoena. We've got to be careful with these.

>> RYAN MEHM: Lorrie, do you have any further thoughts on this?

>> LORRIE FAITH CRANOR: Go on to the next.

>> RYAN MEHM: Okay, we'll go to the next question then, which will be for you, Lorrie. Let's say a disclosure is provided at the time you download an app and the disclosure says that the app will collect location information, would consumers understand this to mean location at this time or location information over time, and would this be material to consumers?

>> LORRIE FAITH CRANOR: Well, from the studies in which we've asked consumers about location, they don't have a good understanding of what it means. So I think different consumers would think different things, and it would be fairly inconsistent. And would it be material? Well, yeah. If we're expecting people to make informed choices, they need to actually be informed about what they are deciding between.

>> RYAN MEHM: Okay. We are running short on time. It looks like we have about seven or eight minutes left, so I want to give each panelist one minute to describe the number-one thing that should be done immediately to improve mobile privacy disclosures. Let's start at the end with Kevin.

>> KEVIN TRILLI: I'm gonna cheat and do two. So, I think the -- the first step by the Attorney General to require policies is a good first step, but I think that would be sort of not a good result if that's all he did. I think the app platform gives publishers or app developers who own more control of the consumer experience, more power to really control the redeployment of privacy policies from a fundamentally different way, just like we saw privacy policy ends up on every Website for whatever 10 million sites. It's starting again now, and I think if we just went to the "text policy" link that we have on the web, I don't think we're being successful. So I think some effort to really at least improve it the next level up would be critical, and that's a very broad consortium group of participants to figure this out. But I think the timing is right here waiting for us. And if we blow it, I think it's a missed opportunity. Second, this whole discussion around data sharing with third parties, I think -- the AdChoices -- I think, you know, we got to keep in memory that it is only 2 or 3 years old. You know, consumers need to see it a few times, understand what it is, and, you know, over time, they're gonna understand what it is. A similar program is needed for mobile apps because we all know there is not cookies in mobile apps and a whole different framework of UDIDs and Mac address. And I think that can naturally flow. There are technological issues that make it a little less straightforward to do that, but I think the similar concept can happen in the last 12 to 18 months. But I think both of those are unique opportunities for the app space. It's a much more rich environment for innovation in the layering or the transparency and notice framework. And I think there's a great opportunity for everyone to do something here.

>> RYAN MEHM: Thanks. Sara?

>> SARA KLOEK: Our developers want clear and concise guidance, And then then want to be done with it. They want to continue to innovate, make cool things. Privacy will be in their design and going forward, but they just -- then want to innovate. They don't want burdensome regulations.

>> RYAN MEHM: Pam?

>> PAM DIXON: I'd say, if I to only say one thing, I think it's just important to think of really approaching a consumer as a whole person, so really thinking cross platform online and off and all the different ways that a consumer can be communicated with. Even if it's just an indirect

communication, have the direct communication within the application or ad or platform. But also, think about indirect through other communication means that are a little more permanent brand pages and so forth, brand communications.

>> LORRIE FAITH CRANOR: I'd like to see the app platforms provide hooks for privacy metadata and require the app developers to supply that in their apps and have the app platforms not only requiring it, but then also expose A.P.I.s that allow developers to actually make use of that data for innovative things in their apps and platforms.

>> RYAN MEHM: Jim.

>> JIM BROCK:I agree with everything that has been said and would say them all myself. I think, clearly, the app marketplaces have a great deal of leverage, but I would emphasize again the importance of them helping push developers to make more educated decisions where the rubber meets the road, which is on the server and where the stuff is stored and where the stuff is often shared. And I think that will happen if they just start to press privacy more to the developer as part of uploading the app.

>> RYAN MEHM: Ilana.

>> ILANA WESTERMAN: Yeah. I think, for us, really wanting to be able to continue to innovate, I think our research really shows we're not there yet. But that's 'cause I think we're just getting started. I mean, if you go back 10 years, look at e-commerce and try to buy something online and how hard that was to do, now how easy it is to do -- maybe too easy. But we can get there through good design, but I think we can't force designers to say, "You're gonna put a checkbox here or a link there." What I think we really want to look at are the underlying goals that we have, what we're trying to achieve. And I know brands don't want to, you know, have their consumers lose trust in them. Then they lose customers. That's not their goal. They're trying, too, to create transparency and control. It is just, I think, we're early stage right now. So we just have to continue to try to solve the problem and work towards those solutions.

>> RYAN MEHM: Thanks. I actually want to ask -- We did so well on that, we've got a few more minutes left. I want to ask one of the questions that came in, either online or through someone here in the room. And the question is, "Can we reach agreement on four or five practices that must be disclosed -- location, for example, sharing with third parties, collecting or sharing other information like contact lists? How do we pick that list if such a list is an advisable idea? Anyone who wants to volunteer on that? Sara, go ahead.

>> SARA KLOEK: Well, since we have existing laws like COPPA, we can start there. Obviously, you have to disclose whether you collect for people under the age of 13. So that's one thing that we can start with.

>> ILANA WESTERMAN: Yeah, I think one of the key things is to look at what consumers care about and what they don't care about, and I don't think we fully have had a picture. But what they care about is consequences and understanding what's gonna happen as you gather that. And so, I think, really, it's less about the four or five things that we need to disclose, but it's more about telling people what that means to them so they can make decisions.

>> PAM DIXON: I think that's right. And, you know, I know that when people contact us, the thing they scream the most about -- There's two things -- location and contact lists, the contact information in their cell phone. They don't want people touching that at all without their permission and probably not even then, unless it is just really amazing and, you know, has such utility that it's okay.

>> RYAN MEHM: All right. Well, I want to thank all of our panelists for being here today. Several literally flew across the entire country to be here. I want to thank everyone who's in the room, for gutting it out, sticking with us till the end. We're not entirely done. We still have concluding remarks. And I would like to now introduce Mary Engle, associate director of the FTC's division of advertising practices. I want to say one other thing, too, before I forget. We will also be accepting written concepts on the proposals and ideas discussed today. We'll be accepting comments starting today and through July 11, 2012. And those comments will inform whatever follow-up results from today's workshop. So with that, I'd like to turn it over to Mary.

>> MARY ENGLE: Thank you, Ryan, and good afternoon, everybody. In keeping with the theme for today, I promise to keep it short. I just want to thank all of the panelists for their wonderful presentations and the discussion we had today. It's been a really educational experience for me and the rest of the FTC staff. One thing that we heard a lot today is that context matters, that it's really what needs to be disclosed, and how it needs to be disclosed, really, is gonna depend upon the particular device -- the consumer, maybe the product, maybe the offer. And we heard a lot -- "It depends." But, of course, the job of the FTC here -- What our goal is is to provide guidance and not just say "It depends." We want to eke out as many black-and-white areas as we can from all these shades of gray that we heard discussed today. We also heard that it's important to take into account typical consumer behavior in a particular online or mobile environment -- for example, where they look on the page and whether or not they will click on a link. We heard the view that platforms have to adapt to the law and not vice versa so that if it's not possible to run a non-misleading ad on a certain platform, then that platform shouldn't be used. We heard about the need for clear and attention-getting labels on links that convey the consumers the significance of the link. We heard about the desirability of modifying or even limiting a claim itself so that maybe a disclosure isn't needed in the first place. We heard a lot of agreement that appropriate disclosures will also often make the consumer experience a positive one in connection with the brand. We heard that the timing of when disclosures are made is very important to whether consumers will really attend or get the information. We heard a lot about the potential use of icons or abbreviations. The question there will be whether consumers understand those icons or abbreviations and who is gonna be educating them about that. We heard a lot about the importance of finding the right balance between the providing enough information and not too much information that consumers are overwhelmed. So I want to -- That was in no particular order. We'll be taking this all in. As Ryan said, the commentary will remain open another six weeks, till July 11. And we look forward to any additional comments you may have, and there's no timetable for the output of this conference. We hope to have something outside the Fall, though. Thank you very much. [Applause]