>> Maneesha Mithal: Okay, why don't we go ahead and get started? If people could take their seats, I'm gonna introduce the fourth panel. My name is Maneesha Mithal with the Federal Trade commission, and my co-moderator is Laureen Kapin with the Federal Trade Commission. I'm gonna introduce the panelists in a second, but before I do, I just wanted to say a word about the format of this panel. We're gonna be discussing the policy implications of both facial-recognition and facial-detection technology. And the format is gonna be a little bit different. We've heard a lot of amazing presentations on the previous panels, but we're not gonna have any set presentations on this panel. It's gonna be pure, moderated discussion, Q&A. I'm gonna ask the panelists if they'd like to speak. Please raise your name tent. For some of the questions, we might call on specific panelists. For other questions, we'll throw it open to the group. Please raise your name tents. And please keep your remarks brief. We have a lot of people on this panel, and I want to make sure that everybody gets a chance to speak multiple times. So, with that, let me introduce the panelists. So, going from right to left? Yes, right to left. We have Dan Solove from George Washington university. We have Simon Rice from the U.K. information commissioner's office, Dan Caron from the office of the privacy commissioner in Canada, John Verdi from EPIC, Erin Egan from Facebook, Pam Dixon from the World Privacy Forum, and Joseph Atick from the International Biometrics & Identification Association. So, I'm gonna just turn the panel over to Laureen for the first half, and I'll take the second half. Thank you.

>> Laureen Kapin: Great. So, I thought we would start out by discussion of the legal landscape. And I thought we would start off with you, Mr. Solove, and talking about the U.S. perspective, and then we'll move on, since we have the benefit of international perspectives here, also.

>> Daniel Solove: Well, it's fairly hard to kind of get a very clear picture of how the law intersects with facial recognition because the answer is it depends. It really depends on what is being done with the information, who is using the information, who has the information, what type of information it is, and kind of whether it falls in the various patchwork quilt that is U.S. privacy law. I think what we see is the legal infrastructure, if I had to generalize. We have, I think, a fairly rickety and kind of incomplete legal architecture to which facial recognition would fit in or interject

with, with a lot of holes and areas where there would be very little, if any, legal protections or regulation. So, effectively, someone could use facial-recognition technology without a privacy policy and ultimately wind up with no regulation at all or no legal restrictions at all. If they have a privacy policy, then there could be some enforcement there, if they violated that policy by the FTC. Also, when it comes to the data used in facial recognition and government access to that data, the law is I think quite lacking in that area. So, under the Fourth Amendment, there's generally no expectation of privacy in public places. Right now we have a case before the Supreme Court, Jones vs. the United States, talking about GPS surveillance, how can you track people with GPS surveillance. Does that give rise to a Fourth Amendment interest? Will the Supreme Court carry its what I think is tortured logic to its conclusion, which is that there's no privacy in public, no matter how pervasive the surveillance is, whether it goes through a GPS device for 38 days to months to years to an entire person's life. What about facial recognition, which could be almost like tracking someone's movements? Will the Supreme Court give us a clear rule? I puts odds at one in 1 in 100 that the court will give us actually anything clear. It will probably decide something narrow that ultimately doesn't really resolve many of the issues, which is really the data, not necessarily GPS devices, but it's about the idea of do people have a privacy interest in where they go and their location. That's sort of the broadest issue. I think they do, and I think there's a lot of risks, things that we could lose, such as practical obscurity and anonymity as we go about our lives was this. And the other thing is the third-party doctrine. Access to information held by a third party is not protected by the Fourth Amendment, according to the Supreme Court. And so all the databases, all the data that's collected about people in databases that would be associated with facial recognition, either the databases that get about people's preferences and whatnot that then get linked up to their identities, to their image, as well as the data collected about someone's facial patterns. All that could readily be accessed by the government with a mere subpoena and can be readily transferred with very little limitation. So I would say that the current state of the law is rather weak when it comes to this. And I could go on, but I'll try to keep this brief and keep that a brief generalization. And it's very hard to answer, too, because it really does cut -- certain industries are more regulated than other industries, and depending on how the system is set up and what information is collected, could really change the equation a bit. But as a general matter, I think, you know, is the law ready for facial recognition? Not even close.

>> Laureen Kapin: Okay. Well, thank you for that. I heard the terms "rickety," "incomplete," few constitutional protections. Let's hear from Dr. Rice from the U.K. And if we can keep the focus on commercial uses, that would be great.

>> Simon Rice: Thank you. Is that on? Yeah.

>> Laureen Kapin: Yeah.

>> Simon Rice: Well, I may be coming at it from a different point of view, 'cause in the U.K., but also part of Europe, there is a piece of legislation that exists and governs the use of personal data. Talking about that, what is the personal data itself? So if you've got a photo of me and you can identify me, that is personal data, so all of the legislation and controls around that will apply in sort of the facial-recognition case. But just to clarify a couple of comments heard today talking about identifiable and what that is, that's more than just putting my name to a picture. If you can target me in some way or change my behavior in some way, that's also personal data. So if I come into a store and you say, "Well, actually, you've been in five times this month already. Here's a coupon to target the things that you've bought," that is personal data. But, also, think about reidentifying, as well. Are you just taking a picture of me every time I come in in order perhaps I do something wrong so then you can go back and trawl through historical data to try and reidentify me and capture that? Again, that would come under sort of personal data.

>> Laureen Kapin: So how is that protected, Dr. Rice, in the U.K.?

>> Simon Rice: Well, fundamentally, I would need to know how that's being used and what sort of processing, storage, taking the pictures off. it's got to be sort of fair and lawful is the notice behind it. I've got to know it's going on for a start, who is taking these pictures, how they're being stored, but also got to know that the requirement for the companies to keep that secure, to make sure it is physically protected so it can't be stolen, lost, or damaged in any way. But also talking about the transfer of that data. That's got to be held quite securely. We've heard instances today about processing off in the cloud. You know, that, by its definition, involved the transfer of that personal data, which is tight controlled sort of outside Europe. But, also, there's the subject, the data subject.

I've got rights where I can come in and demand you stop that processing, object to the type of processing that you're doing, and, also, you know, find out what data you hold about me. So there's quite a few sort of strong rights for the subject in that case.

>> Laureen Kapin: Thank you. Daniel Caron from Canada, can you give us the Canadian lay of the land?

>> Daniel Caron: Yeah, sure. So, in Canada, we do have a federal, omnibus piece of privacy legislation. Our office oversees two pieces of legislation. One applies to the federal government, and the other one applies to private-sector entities that collect, use, or disclose personal information in the course of a commercial activity. So, the act is based on Fair Information Principles There are 10 privacy principles under the federal legislation, and they're loosely -- or they are based on the eight OECD principles, and we add two of them. We term it as a privacy statute, but it is a personal-information-protection statute, and one of the threshold issues is that we have to be dealing with personal information, which is a very, I think, relevant distinction in the context of what we're discussing today. For example, when we're talking about face detection, are we talking about personally identifiable information? Are we talking about personal information? I think it's an interesting threshold issue, that hopefully we'll have the chance to discuss further today. But that's one of the threshold issues as to whether our act applies. Now, assuming we're talking about personal information, then a whole host of obligations apply. You have to be as an organization that's collecting, using, or disclosing the information, you're accountable. You have to have someone responsible. You have to have a privacy officer. You need the informed, knowledgeable consent to the use of that information, and that means you can have expressed consent. You can seek expressed consent, or, depending on the type of information and depending on the circumstances, you can imply consent. And this consent obligation applies across the board unless there's a specific exemption. There's a list of specific exemptions under the act to the consent principle. You have to identify the purpose clearly. You have to say why we are collecting this personal information. You have to provide access upon request. You have to have proper safeguards. You need to be open about your personal-information-management practices. You need to have some sort of a document, a privacy policy, that says, "Here's how we use your

personal information." So basically, we have an omnibus, private-sector piece of legislation that would cover this.

>> Laureen Kapin: Great. I appreciate everyone's specificity. That's very, very helpful. So, now what we want to do is apply what we've heard about the legal landscape and also people's policy concerns to an actual situation. So for this purpose, we're gonna be focusing on facial detection, and I'm gonna give you our scenario, which has to do with a digital sign. So, our setting is going to be SaveMore, a popular retail discount chain. And in SaveMore, there are several digital signs installed, equipped with cameras throughout the store, and the information that can be detected on those signs is an individual's approximate age and gender, and then there's certain actions taken by the sign in response to that information. The signs can display a targeted ad, and if a person is captivated and stops, the sign can generate a coupon. So, our first set of assumptions in this scenario is that the signs only detect age and gender. No data is retained. So, I'm gonna start with the first question, and I'll throw this out to the panel, so if anyone who wants to respond, just raise a sign or a hand. Is there any situation in this scenario where SaveMore should not have to notify its customers of what's going on in the store vis-à-vis the cameras on the digital signs? Any situation where notice shouldn't be required? Oh, I feel like a schoolteacher with no volunteers, so I'll have to volunteer someone. Mr. Verdi, what do you think? [Laughter]

>> John Verdi: Thank you very much for volunteering me. [Laughter] It strikes me that this scenario, because it is hinged on, you know, no creation of biometric, failure to retain data, et cetera, et cetera, et cetera, it starts to look like, "Well, this must be a scenario in which the store can simply go about its business and not disclose anything to anyone." But I don't think that's the case, and what I view it as is a logical extension of what comes up in the fact pattern later on, which is a version of their customer-loyalty program. You know, you invite customers into your store. You're giving them discounts or displaying advertising based on particular criteria. There is certainly I think an obligation on the part of the store to be transparent about how they're operating that program and why you're getting a better deal than the person who walks in behind you. That isn't to say that the source shouldn't engage in the program, but it is to say that they ought to provide notice to customers and be transparent about it.

>> Laureen Kapin: Okay, so there should be transparent notice. And I see Ms. Dixon. Would you like to comment, as well?

>> Pam Dixon: Yeah. I think this brings up the issue of passive consent. If you've walked into an environment, well, you must realize that this is occurring, so therefore there's some form of passive consent that can be presumed to exist there. I think that it's going to be important going forward, looking toward the future in our crystal balls, that we make sure that consumers do not have a privacy environment of passive consent. I think it's the wrong way to go. The rabbit hole on that one doesn't lead to a very good place. So, given that, I think that the best approach would be to have notice that's complete, notice that's honest, a la Beth Givens' remarks today, no language that's euphemistic, saying, "Oh, we're managing our security here." Say what it's doing, give consumers access, and if the collection of data is ubiquitous but not retained, make sure the notice is equally as ubiquitous as the data collection. And find a way to make that meaningful. So, for example, just listing a website is probably not ultimately going to be incredibly meaningful. So I think that it's going to be important to find a new way, or perhaps an additional way, of providing consent -- or, excuse me, notice in that situation.

>> Laureen Kapin: Okay, well, following up on that --

>> Joseph Atick: Question.

>> Laureen Kapin: Great minds think alike. I was just gonna ask you about this.

>> Joseph Atick: Okay.

>> Laureen Kapin: Maybe you can also focus, besides what you had in mind, on how that notice can be most meaningful in terms of where, in terms of content, et cetera?

>> Joseph Atick: I mean, another dimension of this is not only notice is gonna be important, but also the locus of operation is gonna be equally important. I mean, if you are creating a situation where you're operating distant environment where the consumer does not have any choice anymore,

because now you're putting signs in this area, and you're saying, "Okay, my choice is not to go to the store, but this is the only store on the block where I can find medicine or I can see it open 24 hours a day." The locus of operation becomes a critical element in creating an acceptable environment. And in that, the criteria should be does the notice provide still the consumer with adequate choice if they choose not to participate, if they choose to avoid that area? And in some cases, it does, in which case we would feel comfortable that that is a legitimate application. In other cases, this would definitely hamper their ability to conduct their day-to-day lives. We cannot penalize people just basically because they choose to remain outside the realm of being targeted.

>> Maneesha Mithal: Can I actually ask a follow-up? And I see Simon's tent is up, but I just want to follow up on your point, as well as Pam's point about passive consent. So, I think here we're talking about facial detection, no retention, just collecting age and gender. And just following up in the passive-consent point, I wonder if there's an alternative. Somebody earlier on mentioned you don't have to come into the store if you don't like this practice. Is the only alternative to not use the cameras, or what's a real alternative to provide consumers with actual choice in this situation? So, I'll let Simon speak first, and then if somebody could address that question.

>> Simon Rice: Thank you. I think going back to if there was a situation where a notice wasn't needed, the only way I could image that occurring is with some sort of covert camera that's not noticeable, 'cause surely a display with a camera in it is a form of notice. You can see that it's happening. So therefore, it's covert, and people are gonna get suspicious, and then your transparency and trust of your consumers has gone completely, in which probably you end up in a worse situation. Think about how can you get consent. I mean, obviously, you could press a button, and then the advert appears. You can provide two entrances to a store. There are ways around it. And, again, we've thought about the location of that store and say, "Well, if that's the only store in the block, well, that's quite a problem." But, also, if you think about maybe an airport. People want to travel. You only actually find out that those displays are happening once you actually get to the airport. Do you really have a choice? Then, obviously, the consent model breaks down if you don't have that choice.

>> Laureen Kapin: Mr. Caron.

>> Daniel Caron: Just very, very briefly. Surely, the idea of having a sign outside the store that says, you know, "such and such technology is in use for this purpose," is probably a starting idea. But maybe there's, depending on the technology, I mean, depending on how wide the camera angle is, for example, maybe -- I'll make a reference to ice hockey. You can have sort of the goaltender crease, if anyone follows hockey. [Laughter] You have, like, sort of a red line that delineates --

>> Laureen Kapin: You're gonna have to explain that one, Dan. [Laughter] Sorry.

>> Daniel Caron: Anyways, wouldn't be a Canadian on the panel without an ice hockey reference. [Laughter] It's really a red half-circle around the net that delineates where the goal crease is from the rest of the ice. Maybe one idea is having an area delineated saying if you cross this line, you will be subject to facial-recognition technology, so don't cross this line. Crossing this line constitutes implied consent to "X," "Y," and "Z." So I think just limiting it to signs is maybe not opening up our minds enough to other possibilities that exist as to getting meaningful consent, whether it's inside a store or outside a store, for example.

>> Laureen Kapin: Oh. Pam.

>> Pam Dixon: Oh, thank you. Yeah. The walkout opt out is just not credible in an environment of ubiquitous collection. How much are consumers going to be asked to walk out of? So I really would have to protest the walkout opt out as a nonviable option in the long term. Since this is a forward-looking panel, if we look down the road 10 years, we shouldn't have to live in an opt-out village. [Laughs] So we've got to avoid that fate.

>> Laureen Kapin: Okay. So, I'm gonna change our assumptions a little bit, and I'm going to add the fact that SaveMore is gonna retain that image, with the information being retained being the approximate age and gender information, so they are gonna retain that information. Should the notice and consent policies of the store change? And maybe we can focus a little bit on this opt out. We've heard some objections to the Walkout opt-out scenario. What would be other forms of opt

out that would be more meaningful or more protective of individuals' privacy and choices? Mr. Solove.

>> Daniel Solove: Yeah. I actually want to build from the first problem, because I actually think the first instance doesn't trouble me as much. I might sound like a privacy heretic. This next variation, and it starts to trouble me. 'Cause ultimately, I begin by saying "What is the problem?" And I use "problem" rather than "harm," because I think "harm" is kind of loaded up with a lot of baggage. But is there a problem with certain kinds of facial-recognition technology? If it's not retained at all and it doesn't really identify a person, it just captures a few details about them, is it any different than just a person standing in front of a store? You walk in, and they look, and they get a rough estimate of your age, and they can probably figure out your gender, and they just decide to hand you a coupon or not. Is it any different than that, and what is the problem with it? I think that it becomes a lot more serious problem when obviously this could cause chilling effects, depending on the context and others, but I don't see that in the first scenario. The second scenario starts to trouble me a bit more, because now you have data retention, and this data could -- at least it could potentially, you know, become identified information about an individual. Right now, it seems like it might not be enough to identify an individual, but it's certainly components to which if you add other data fields, it could start to become able to identify a person. And that, then, gets into a zone where I think you need some greater protections, especially when this information is kept and later on it might be used or it might become something that could eventually attach or fix to particular individuals. At that point, then, I think we need to deal with issues about security and secondary uses and a pretty robust regulatory scheme beyond notice.

>> Laureen Kapin: Okay. Mr. Verdi, I saw your sign up first.

>> John Verdi: Question about the hypo.

>> Laureen Kapin: Yeah. [Laughs]

>> John Verdi: Is the age and gender retained as a unique entry, or is it aggregated? Is it just aggregate statistics?

>> Laureen Kapin: It's aggregated.

>> John Verdi: Okay. Oh, okay.

>> Laureen Kapin: For analytics, for example, I think we saw that example earlier on where these reports are then generated. Here's the number of females and males that pass by the sign. Here's how long they paused. Here's how old they were, et cetera. So, Simon.

>> Simon Rice: well, maybe my original response was assuming that we were aggregating so far.

>> Daniel Solove: Mine was assuming not aggregating either.

>> Simon Rice: Jumping ahead to the worst-case scenario.

>> Laureen Kapin: [Laughs] But if you'd like to talk about the scenario you're talking about, go right ahead.

>> Simon Rice: Certainly now we've got that retention of data and personal data. That clearly has definitely gone into that case of, yeah, we are processing, so now, in the U.K., Data Protection Act has kicked in, or the European Directive. So therefore, all of these obligations of security and rights of access are then also kicked in. And, also, one of those is strictly around determining the processing and the thing. You know, once you've given me a notification, say this is what you're gonna do with my data, you can only do that, and this function creep can't come in.

>> Laureen Kapin: Okay. Ms. Dixon.

>> Pam Dixon: Yeah. I think for me, when I'm thinking of the differences between digital signage, for example, that's just doing, you know, gaze tracking or something like that and actual facial recognition and retention. There are differences, and they're substantial, and they're meaningful. But here's the deal. And this is where I think we've got to be careful of process. There are going to

be more hybrid viral environments than non-hybrid environments. So, for example, in the deployments that I've seen, digital signage is deployed alongside facial-recognition technologies alongside security installments. So these are three different functions of all technologies that are doing some very similar things. So procedurally, for a company that's doing this, whether it's a private retailer, a public space like a mall, an airport, et cetera, there's going to be a certain process that they have to go through to decide policy. And my concern is that that process needs to have a lot of integrity, and we can't just give away a whole bunch of stuff on the front end, because it tends to impact the back end, too. That's why we'd say we've got to be careful even when we're not retaining so that there's a good procedure in place throughout.

>> Laureen Kapin: So, I want to make this a little more problematic. Now I'm gonna give you some assumptions where the image and age and gender are tracked, and they're shared across multiple signs, okay? So someone going in the store may stop in front of the first sign. It's detected t they are female. They're in their 30s. And out comes a coupon for macaroni and cheese. That person goes to the next aisle, and that information is transmitted. It's the same image. Out comes a coupon for Frosted Mini-Wheats. Does that change your analysis, Mr. Atick?

>> Joseph Atick: Well, actually, in order to understand the different shades of gray that you've proposed in your different analyses, I think we need to take one step back and understand that there's one key element in these whole processes that we ought to be spending more time discussing, and that is what we call the face print. It was mentioned earlier in this previous session. The face print is ultimately the element to that allows a system to perform the identification of a person or even to temporarily know that this person is the same person that was in aisle three versus aisle seven. So if we begin to elevate the face print to the status of a PII and acknowledge its ownership to say that while my image may not be owned by me and can be taken by anybody in public, because my reasonable expectation of privacy doesn't exist, my face print is supposedly an element, a unique code, that belongs to me. And therefore, if you are to exploit it in any way, by storing it in a database, you need my consent. By temporarily generating it and matching it against another instance in the last several hours, you need my consent. Therefore, in all of the analyses that we've heard today and the parting point for the International Biometric Industry Association has always been recognition of this code as the most critical element that needs to be protected. Therefore, in

your scenario, you're now starting to generate a face print. because image-to-image comparison won't work, as we know, in order to determine somebody's identity and know that it's the same person. We have to go through a process of going into a face print. And therefore, every scenario of complexity that you talk about can be resolved and addressed if you give the consumer the control over the face print and say no application can exploit the face print without my explicit consent. And therefore, if you're proposing an application that does that, you should seek my consent. Some of the applications that Facebook was talking about, or face.com and others, do get my consent, and therefore, there is no problem. But in the store, where this is an application, I'm not sure how you're getting my consent. You're generating my face print, exploiting it for some commercial purpose, and it's almost like a copyright. It's owned by me. So we see this as a problem.

>> Maneesha Mithal: I just want to follow-up on that, just to see if there are any analogies between the kind of offline world and online world. One of the things that we put out in our preliminary privacy report is that, for example, contextual advertising where it's just kind of serving an ad based on the content the viewer is looking at at one point in time doesn't raise the same concerns as behavioral advertising, which is essentially capturing a person's movement over time. And I think the difference in the scenarios Laureen was just positing is the first scenario is just not retaining information, serving a contextual ad, in a sense, maybe. And I just wonder if there's any different considerations. You're suggesting that the face print may be a different consideration than something that happens online, and I just wanted to explore that a little bit with the panelists.

>> Joseph Atick: But you couldn't generate the scenario that Laureen was talking about without going through a process that at least temporarily generates a face print.

>> Laureen Kapin: Okay. I have a very interesting question here to evolve the hypothetical even more. Here's the additional facts. Others around you can see what advertisement is displayed, so this is a really big digital sign. And the sign's gonna evaluate your age, gender, and emotional state. And you are now being offered, because you seem a little down, some anti-depression medicine, an ad for some antidepressant medicine or some wonderful diet supplement that can transform your

mood. So how does that change your assessment of what type of notice and consent people should be given in that situation, Mr. Solove?

>> Daniel Solove: Well, I still assume that if no information is being collected in a situation and someone is in the store and it reads them, besides, you know, it might be creepy and not a wise business practice, and it might anger people to see this thing flash up, but beyond that, I really don't see -- You know, it's basically doing a sensing of what anyone else would really sense. It's just doing it technologically. And so I hate to sound like a privacy skeptic, but, you know, I go to the automatic sinks, and I put my hands in, the water comes on, and I go, and I touch, the thing comes down. And so if a sign, you know, lights up for some reason based on, you know, something of the way I move or how I look, if it's not storing that information and not revealing something about me that anyone else around there would have already been able to observe, I think then it doesn't -- I don't know what the problem is, other than creepiness or annoying. It starts to become a problem in my mind when information starts being retained or it's detecting certain things that other people around me wouldn't be able to detect, and then it 's starting to reveal certain things about me that otherwise wouldn't have been revealed. That's when I get troubled. But otherwise, I really don't see the difference.

>> Laureen Kapin: Okay, Pam.

>> Pam Dixon: Yeah. I think Dr. Atick has proposed something I think very intriguing. And basically, what it does is it shifts the frame for the policy analysis. And I think it deserves exploration, because, Dan, I think what you're proposing is what I would call a very traditional kind of privacy-framework analysis. And I think what Dr. Atick is articulating is something that's quite fresh and new, and I would be very interested in pursuing that further and seeing where that goes. Because I think that the idea and the motion of having the -- I would call it maybe the development or attenuation of a new form of PII born of technology, it deserves further consideration.

>> Joseph Atick: And it shifts the responsibility of protecting the identity not on you, but on someone who's exploiting that identity. Therefore, they are subject to liabilities that exploitation of property could fall under. And so it creates a different kind of case law that is not necessarily

constitutional in its form, but it also creates a liability that may chill down some of the zeal of creating applications that might invade people's privacy.

>> Laureen Kapin: Dr. Rice.

>> Simon Rice: I mean, just to pick up on that, once we, you know, bringing in this medical-type data, this emotional state, that's clearly taken us into the case of sensitive personal data. And therefore, the only legitimate basis that SaveMore have got for doing that processing would be my explicit consent.

>> Laureen Kapin: Although it is just based on someone's facial expression. It's not any invasion of their records.

>> Simon Rice: No, no, but it would be presenting that information around and assuming they're gonna have a very good accuracy rate. 'Cause otherwise, why are people buying this advertising?

>> Daniel Solove: What if a human saw it, and I stood there myself, I looked at your face, I saw that you were happy, and I just doled out the coupons? Would that be different? And I retain it. Actually, I have a better memory. The machine forgets, but I actually have a memory.

>> Simon Rice: Well, in that case, no, because it wouldn't be any automatic processing within the computer or processing that within your mind.

>> Daniel Solove: And what would make the automatic processing particularly problematic as opposed to mine? 'Cause in a way, I then could have actually more retention in me than the machine would?

>> Simon Rice: Just the way that the legislation is put together. It can only be done by automatic processing would then the legislation kick in.

>> Laureen Kapin: Pam.

>> Pam Dixon: Yeah, I think that certainly a partial answer to that query is the nature of the digital signage itself. So, for example, the Tokyo forms of digital signage are quite broadcast in nature. Some of the signs are an entire story and building-high. So I don't think that a person handing me a coupon or trying to spray me with perfume annoyingly... [Laughter] They may be annoying, but, Dan, I get your point, and I see it. But I do think there's a different nature to these signages, and I think that there's a certain shame element that when you -- and actually, we've done this. We have a nice video where we wanted to post today, actually. But we interviewed people about their responses to some of the signage, and some of them were ashamed of their age and things, and it documented these qualities that they viewed as ephemeral in face-to-face interactions, but is more permanent in electronic interactions. And that's just I think part of being human.

>> Laureen Kapin: Hmm. That's very interesting, those distinctions. I'm gonna add a fifth assumption here. Customers that choose to flash their brand-loyalty cards, they can receive coupons that are worth more than the customers who don't. And these loyalty cards, as you may realize, they can transmit individually identifiable information, such as that person's name, address, age, and e-mail. That's all keyed to the card. So in that situation, what type of notice should SaveMore be giving to its loyalty-card holders? Mr. Verdi?

>> John Verdi: I think at that point is where you move into meaningful consent. The consumers need to meaningfully opt in to this sort of process. And if they find the process to be valuable, they will, and if they find the process to not be valuable, they won't. But you don't just get away with notice or notice and, you know, opt-out consent on this basis. You know, you don't just get to do the facial recognition and then make a determination, "Aha, this person is a loyalty-card holder, and unless they opt out, I'm gonna make this link and go ahead and give them more valuable coupons. It's meaningful opt-in consent to this sort of program. And if you like it and enjoy it, God bless you, and if you don't, Got bless you, too.

>> Laureen Kapin: So when should that happen? Can we make this a little more concrete?

>> John Verdi: Sure. Well, I mean, I think there's a couple of places that it could happen. I'm not gonna tell SaveMore how to run their business, but I think number one --

>> Laureen Kapin: Oh, go ahead. [Laughter]

>> John Verdi: If this process is up and running and someone decides to sign up for a loyalty card that day, it's fairly easy to demonstrate the technology and explain it to folks and go ahead and get their opt-in consent for it. I think that you have a slightly messier, though not insurmountable issue, with existing loyalty-card holders. And from there, it's a matter of making sure that the opt-in consent is meaningful. And if you can do that for existing loyalty-card holders, that's great. I think that what you don't want to do is go ahead and opt everybody in to it, wait for your customers to object a lot, wait for EPIC to file an FTC complaint, and then roll the change back and have your C.E.O. apologize. [Laughter]

>> Laureen Kapin: Fair enough. Dr. Atick?

>> Joseph Atick: Just clarification. When you said there is no face recognition involved here, there's just somebody has a card, and they would have to use their card to present it to the system in order for them to get that coupon, so in a way, there is already a meaningful consent in some way, which is if I don't want to get that additional coupon, I keep my loyalty card in my pocket. It's not RFID, so it doesn't protect me from a distance. So I don't see the scenario any different than somebody just keeping it in their pocket and not presenting it to the system. That's a form of an opt out.

>> Laureen Kapin: So people could just opt out by not electing to use their brand-loyalty card.

>> Joseph Atick: Exactly. I mean, you're not assuming that they are doing it at the checkout. You're assuming that they're doing it at the point --

>> Laureen Kapin: At the sign.

>> Joseph Atick: In which case, if they are supposed, they could get the low-end coupon without presenting their card. They can do that. Otherwise, they can present their card and get a higher coupon. So this case, we see not any different, in my opinion, in the previous scenario.

>> Laureen Kapin: Although even though there's not facial recognition, it now is, through the use of the loyalty card, linked to a specific individual, and that specific individual's information can then be shared with third parties, for example, to generate high-value, personalized coupons.

>> Joseph Atick: Right, so keep the card in your pocket. [Laughter]

>> Laureen Kapin: Mr. Caron?

>> Daniel Caron: One point of clarification, when the customer is flashing their brand-loyalty card, are they also flashing it next to their face, or are they just flashing --

>> Laureen Kapin: It's a separate reader.

>> Daniel Caron: Okay. Irrespective of whatever scenario, I know under our federal legislation, clearly there is a collection of what would be personal information, so all of the privacy principles would apply. So the question of knowledgeable consent would kick in, the question being, "Well, how and in what way we might obtain that consent?" Well, again, you might have a problem description on the camera saying "if you flash," you know, for individuals that flash your card, you know, "it may be used to give you a higher-value coupon." It can be described in the privacy policy, not only as a matter of ensuring that you have meaningful consent, but as a matter of openness, which Is another principle under our legislation.

>> Laureen Kapin: I have one last question on this scenario with digital signs. We've touched on this a little bit. But are there any locations where this should just be banned? I think, you know, bathrooms, locker rooms, medical facilities were mentioned. Are there any other locations that should be off-limits for digital signs? Ms. Dixon?

>> Pam Dixon: Yeah. It seems straightforward, but it's actually not that straightforward, because the people who are walking around digital signs are usually in hybrid environments. So, for example, the grocery store like a CVS or a Walgreens, it has a minute clinic. You know, the McDonald's that has a digital sign with the kids' playground. How are you going to segregate, for example, information that would in an online context be subject to COPA regulation, from, you know, basically kids' information. How would you segregate that? And Let's just talk about a store context. You're in one of the stores, like a CVS, and they're collecting data. And at one particular aisle, gazes on a particular shade of lipstick or brand of shampoo. What if there are over-the-counter medications right next door to that? How do we segregate some of these broader medical uses? It's really actually a tricky, tough question. But broadly speaking, I think that it will be very important moving forward to define what constitutes sensitive information, certainly HIPAA compliant, certainly children under the age of 13. I think we can agree on those. I think places where there is not a lot of choice about being there would also probably, you know, qualify. But that's contextual. Each person may have a different definition of what's necessary.

>> Laureen Kapin: Mr. Verdi?

>> John Verdi: As to sensitive areas where they shouldn't be installed, are we talking about facial-detection signs or facial-recognition signs?

>> Laureen Kapin: Facial detection.

>> John Verdi: Facial detection. Okay. Then I'll hold my comment for the facial recognition.

>> Laureen Kapin: Mr. Rice?

>> Pam Dixon: I was applying it to both, by the way, not just detection.

>> Simon Rice: I think it would just have to be clearly linked back to the original purpose for the processing. If it's just for a display sign and it's for advertising, then you can clearly find, you

know, good situations for that. If that was your purpose, then, you know, it shouldn't be in the toilets, in the bathroom, or whatever. Yeah, clearly linked back to the original purpose.

>> Laureen Kapin: Thank you. Oh, I'm sorry. I didn't see Dr. Atick.

>> Joseph Atick: Yes. There is another dimension in this question that I think we ought to explore, which is the pervasiveness of it. I mean, do you want to live in a world where you walk into a mall, hardly 400, 500 yards, and there are a thousands standing outside each door offering you different flashing things at you? It almost starts bordering harassment in a way. Not only location should be addressed, but also the density by which these are used as a dimension. Maybe it's difficult to quantity at this point in time, but the density of these devices could border on harassment. And it's suffice to put it in the context of humans, an army of humans offering you and flashing things at you. Even though they don't know me, it's enough for me to just run out of the mall and not come back again.

>> Maneesha Mithal: Okay. It seems like a lot of people want to talk about facial recognition, so why don't we move on to facial recognition? I have an infographic up that I'll just walk everybody through, and then what we can do is I want to ask what the specific responsibility of the various players in this change should be. So, sticking with the SaveMore example, let's say John Doe customer walks into the store. There's a camera in the store that takes a picture of him, and the SaveMore sends the picture to a technology company. Let's say this is a facial-recognition technology company. The technology company, as we heard earlier, has to have a reference photo against which to check this photo, checks against the reference photo. That reference photo could be a criminal database. It could be a social-networking site. It just could be through a search engine. And then the technology company spits back a report to SaveMore. The report could just be "this is John Doe." The report could be "this is John Doe, and here's what we found about his interests and what brands he likes," et cetera. And SaveMore shows John Doe a coupon. So, I want to ask what the responsibilities of the various players in this chain are. So let's say that the reference photo comes from a social-networking site. We've talked a lot about SaveMore and its responsibilities. We've talked a lot about notice and choice. I want to bring into the discussion things like privacy by design and other of the Fair Information Principle. And I just want to pose a

question to Erin from Facebook, asking if there's any responsibility that social networks have in this chain.

>> Erin Egan: Yes, and thank you. And I appreciate the opportunity to talk here today, and there's been a lot of discussion today around Facebook, and so I'm looking forward to the opportunity to talk about what we do. Now, in this scenario that you've just identified, this is not a use of facial-recognition technology by us. And we didn't get an opportunity on earlier panels to talk about what it is that we do. Again, we're committed to the social context and privacy, and we have a one-pager that we've put out there so folks can learn more about exactly how we use facial-recognition technology in a privacy-enhancing way. But, so, this is separate analysis, and this is us as custodian where we have photos. People talked about that a lot today, how many photos there are on Facebook, and we take that very seriously when we're a custodian of photographs. So what is our obligation? Well, first, we wouldn't share in this situation. This is not something we do today where we share photos that people put up on our site. So this would be maybe you're talking about in a hypothetical a scraping situation where someone takes the photo without authorization from us. And, again, we prohibit that kind of activity by our statements of rights and responsibilities. But I think it's a multifaceted responsibility, so I think, number one, we prohibit that activity. Number two, I think it's key that we educate users about this. People talked earlier about the fact people are making things public and what does that mean. Well, we have a responsibility. We all have a responsibility to be educating users about the implications of making things public. People need to know when they're doing that what that means, and that's something we take very seriously. So, again, the third is that we will take enforcement actions against folks who actually violate our terms. So here, if they're taking a picture and they're using it in a way that, again, this would violate our terms, we would have a problem with that, and we would take action. So, again, it's a multifaceted response, but the bottom line is that we take this very seriously.

>> Maneesha Mithal: Okay. Okay, and I want to come back to you to talk a little bit about your uses of facial-recognition technology.

>> Erin Egan: Yeah.

>> Maneesha Mithal: But let's do that after the hypothetical. Okay, so, now let's move to the technology company. This would be the facial-recognition technology company. And I wanted to ask Joseph what the responsibilities of that actor in this circle are towards consumers, yes.

>> Joseph Atick: Going back to our responsible-use protocols, first of all, the technology company cannot convert the images, whether they took them from some source through harvesting, scraping, or whatever, they cannot convert the images into face prints which are required to do the identification without explicit consent. The consumer has to say "I agree. You can convert my images into face prints. You can use my face print to target me if you like. But give me value add." And the opt in here is that I'm giving you the right to convert into face prints. Now, even if consent was given, there is a responsibility that lies in the hands of the technology company, because even if you give me the consent, you cannot treat my face print lightly. You have to protect my face print from unauthorized use and, also, the scope of the use. If I gave you consent for an application which targets me for sporting goods, I don't necessarily give you the authorization to be targeting me for liquor or some other type of application. So consent has to be very, very focused, and technology companies have to have technical measures, security measures to protect that valuable element, which is the face print of all the people that have pictures been loaded on LinkedIn or Facebook that have given their images to the technology company. So I think we take it very, very seriously. Protect the database, don't convert to face prints, and no match, no memory. So the live, also, when you're seeing people who are not in the consent list, you cannot save their face prints into your database of unidentified people.

>> Maneesha Mithal: And how do you police against that?

>> Joseph Atick: In fact, the audit mechanisms have to be in place. There have to be audit mechanisms that allow the consumer to reach back and put a liability on the application provider to say "You've used my face print illegally, or you've used my face print without my consent." Whether there is a certification that has to go through an industry association or a government body that can play that role to put a stamp, a seal of approval to say this meets the privacy standards for safeguarding face prints. At the International Biometric Industry Association, which, by the way, all of these issues that we're talking about today were out there 10, 12 years ago. In fact, when we

were founded 14 years ago, we had to deal with them. Some of you may have heard about the Snooper Bowl and some of the implications of use of facial-recognition and surveillance applications. So these issues were addressed, and in response to them, the industry adopted ethical-use measures. And while it was a self-regulating element, if you did not sign to it and subject yourself to the industry association type of vetting, you will not get our seal of approval. And so that's one element. Maybe the scope is much larger than CCTV back 10, 12 years ago, and therefore a certification process has to be more rigid. Many countries that we've been talking to have decided to create privacy bodies that certify applications subject to this type of criteria, and I think we may need them.

>> Maneesha Mithal: John?

>> John Verdi: Just on the enforcement mechanism, one of the things that we are sorely lacking in this country right now, and I think Dr. Rice can speak to its existence in the U.K., is an enforceable, legal right for users to access and examine the data that companies hold about them. Users have this right when the federal government holds data about them under the Privacy Act. But under E.U. law, the policing mechanism is placed largely in the hands of those who have the greatest interest in doing the policing -- the users themselves, the data subjects.

>> Maneesha Mithal: Actually, just following up on that question, I think both you and Joseph raised the possibility of potential enforcement by the consumer of their own rights. But what if the consumer doesn't know that this is going on or the consumer doesn't know the implications of this? I guess that's where notice comes in. Are we putting too much of the onus on the consumer here? Dan Solove and then Dan Caron.

>> Daniel Solove: I think yes, and I think one of the tricky problems when it comes to the kind of notice-consent model with consumers at the helm is it's great that the consumer has this power to do it, and I'm all for that. The difficulty is managing that across all the myriad number of companies that gather the data. You know, it could be thousands. You know, I'm gonna go to each one, learn about that data, figure out things. It'd be a full-time job. I can barely do it now myself, and I studied this. And so it's hard to imagine a consumer with the time and resources to be able to

do this effectively, so we need something else to supplement it. It's great if someone wants to do it, but I think a lot of people are not really up to the task and don't have the time to do it.

>> Maneesha Mithal: Dan.

>> Daniel Caron: On to the other comments, another way to ensure protection is by way of contract. There will be a contract, I assume, doing the store and the tracking company, delineating the terms of, you know, costs and the services that the store wants from the tracking company. Under our legislation, we have distinguished between a disclosure of information between one entity and another and a transfer of information for, for example, processing purposes. You want your information stored on a server. That would likely be seen as a transfer of personal information. And because of the first principle is the accountability principle, the original organization remains responsible for that information and has to ensure a comparable level of protection. And usually the way they do it is by way of contractual terms. So that's another way that the store can ensure protection of the information that it transfers to another entity.

>> Maneesha Mithal: Joseph.

>> Joseph Atick: Yeah. I think we can learn a lot from other experiences where PIIs were deployed, such as in HIPAA and in medical records. I mean, clearly, in those cases, the consumers are not going around auditing the hospitals and their doctors to make sure that they are not violating the privacy of their medical records and the PIIs contained in them. What you find there is that there's a clearly defined liability that makes it very difficult for an organization to treat this as a secondary problem. They become attentive to it. All you need to do is one case where enormous amount of money is being levied in fines against somebody who violates your right to the privacy of your PIIs. And if there is a liability, there will be a lot of law firms out there who will take these cases and will do the necessary work to make sure everybody behaves. I think we learn a lot by treating face prints as PIIs and the associated experience that we have in defining the same -- I mean, we don't think you should treat face prints any different than PIIs. We need a comprehensive metric of what constitutes a disclosure of PII and what happens when that disclosure takes place.

I'm liable because you entrusted me with your PII, just like you entrusted me with your medical records. So we can learn from there.

>> Maneesha Mithal: So, I want to go back to some of the discussions we were having when we were talking about facial detection on notice and choice notice in the store, and it seems like from the comments on the facial-detection discussion that people feel that there should be pretty robust notice in choice, particularly when there's gonna be facial recognition, when that information is gonna be captured to advertise the person, particularly when it's captured over time. And I want to go back to the question of, you know, we've talked about walk-away choice. perhaps not being enough. So what are some alternative methods of choice? I mean, would the consumer be able to turn off the device? We were joking on the call the other day, should the store offer ski masks to the consumers to just hide their face? [Laughter] Should there be an option to blur your face? And one other thing I was thinking of as I was preparing is that, you know, one way you could provide choice would be to have the technology company say, "Yes, this is John Doe." You walk into the store, and the guy says, "Hello John Doe. We can now track you across the store and give you coupons. If you don't want to do that, click here," or have it be an opt in. So in a way, that would get the consumer's attention, so maybe better than a notice outside the store, but in another sense, the collection has already taken place. So I'm curious as to what people's thoughts are as to what form the choice should take.

>> Joseph Atick: There is a simple mechanism to actually foil this whole system -- just keep looking down. [Laughter] Truly, just keep looking down. And you don't have to put a mask on. You just look down at your feet.

>> Maneesha Mithal: The other thing we've heard, I think, is that if you hide your face like this. So we're gonna see people walking around stores like this, with their hand covering half their face. But Simon?

>> Simon Rice: I think the easiest one, you know, going for this full, opt-in choice and the display board doesn't do anything until you walk up to it and press it in some way. You've got to interact with it in order to receive your coupon, so why can't you interact with it before it prints the coupon?

>> Maneesha Mithal: Good thought. Anybody else?

>> Joseph Atick: The power with that scenario --

>> Maneesha Mithal: Dan? Sorry, Dan first, yeah.

>> Joseph Atick: The problem with that scenario is that the power of digital signage is that it attracts your attention, draws you in. If you are to be coming into a static place, and you have to press the button, that whole industry would collapse.

>> Maneesha Mithal: Dan?

>> Daniel Solove: You don't need to maybe, you know, stop processing my personal data in order to grab my attention.

>> Joseph Atick: But in order to target you with an age-specific, gender-specific, profile-specific, even before I know who you are, it's still a prerequisite that they attract your attention before they get your consent, which is the problem with this whole scenario.

>> Maneesha Mithal: So, Dan Solove?

>> Daniel Solove: I think it really turns on purpose of use and how that information is going to be used. Is it just for a coupon? What are the downstream uses? What are people being asked to consent to? Obviously, if a business wants to preserve its ability to use information, it can just say, you know, "Hey, we will collect your thing. We'll give you a nice discount, and then we'll keep it on file and use your face print for future uses that will be of great benefit to you and we know you're gonna love." And they might be a wide class of things, and people are like, "Okay, great. I get 10 cents off of a coupon, I'll do it." I think that's one of the problems is that it's very, very hard for consumers to really understand and assess what those potential future purposes could be down the road, which really gets into some of the difficulties and challenges with the notice-and-choice

model. On the one hand, we don't want to be too paternalistic and say, "No, you know, we will never allow these technologies, and there's no facial recognition allowed period." On the other hand, it can be very, very tricky, even with asking people for a notice, because people will often give their consent because they really don't fully understand, "Oh, I'm just getting a coupon. Oh, yeah, I trust this store. It's Wal-Mart. Would that really hurt me?" You know, they're not going to do anything bad with it. But who knows what's going to happen to that down in the future, what those future uses might be, and if anyone's really, you know, qualified to be able to fully assess and understand the risk involved with that. And that's a real challenge, and I don't know the answer, because on the one hand, you could have the government say, "You can't do this, and you can do that." On the other hand, if you give it to the consumer, you're giving it to someone who might never be informed enough about what those uses could be to really make an appropriate decision at that particular point in time.

>> Maneesha Mithal: Can I ask a follow-up? So, I guess two parts. One is how can you ensure or make sure that consumers are better informed so that they are making meaningful choices. And if you think that in many instances consumers will not be making informed choices, what are some other protections that can be put in place in order to alleviate that concern?

>> Daniel Solove: Well, that's the million-dollar question. That's your job. [Laughter] But my job is just think big thoughts. But I think that you try to notify -- it's one of the big challenges of privacy is the future uses are potentially infinite. We really don't know what they are. And people can write privacy policies and get consent by making some vague promises. You might force in privacy policies, have substantive requirements of being more specific about what those uses might be so that you can't be so vague that the future uses could be potentially infinite. And so if you deep a tighter leash on what those announced purposes are, you can then maybe confine the infinite range to a more finite range and allow people To make choices. The other thing, find some way to educate people about the implications of a particular choice. The difficulty is, you know, some studies show that people really have a lot of trouble in this context making informed choices, even told about all of the potential consequences. And nevertheless, even though we know what their preferences are, doesn't match their choice, what do we do in those situations? How paternalistic do we do when we realize people's choices actually don't even match their very stated preferences?

I don't know the answer to that. I think it involves a lot of study about how people decide and then how best to create rules to get people to make better and more informed decisions about themselves without being too paternalistic.

>> Maneesha Mithal: And this is for the whole panel. And I'm gonna call on Pam momentarily, but just another follow-up. Would data minimalization help alleviate some of the concern? So, for example, I'm gonna track you across my store for the next hour, and then I'll delete your data. So in other words, it's like just for a session am I gonna track you? And Is that gonna resolve the business needs on the other side of the aisle? So, I just throw that question out. Pam, why don't we hear from you, and then if anybody else wants to answer that question.

>> Pam Dixon: Just a couple of thoughts, some stray thoughts here. I think we have to take into account the pervasiveness of this technology. We were just talking about this. When you go into large installations, particularly in Asia, where this technology is much more mature than it is here, it is truly awe-inspiring. And I just want to get across to everyone that the collectors, regardless of their purpose, look identical. So for a consumer to walk into an environment and go, "Oh, well, this is for security. This sensor here is doing facial recog. Oh, and this is just detecting." It's really an impossible task in these more mature, technical environments. We've got to really keep that in mind and try to kind of see that in our minds. And because of that, because of these hybrid installations, I have to tell you, I hadn't thought of it before this morning. I really like Beth's idea of a QR code on these sensors. I think it's a terrific idea and really innovative, and I'd love it if the industry took that and ran with it a bit and saw where it went. I think that's actually a potential solution. Something I'm concerned about here, and I'm again very interested in answers to this. I don't have them. And that's what happens to the habituation of collection in this instance? I'm very concerned about that. I don't know what to do about it, but I don't like the outcomes that I see. I don't like the research outcomes that have been done in academia. We have a habituation factor that's fairly unavoidable. So what do we do about that? I think something is gonna have to be done about notice. We can't put notice on every camera, or can we? Can we limit cameras, or can we? I don't know. But here's some of the questions that we have to ask.

>> Maneesha Mithal: Just following up on that, one of the things, again, that the staff recommended in the preliminary privacy report for online tracking was the idea of a do-not-track. And I wonder if there's any ideas or thought if this becomes ubiquitous, would there be a viability in a do not track my face or some sort of centralized mechanism where consumers could opt out of tracking.

>> Joseph Atick: Your face print is off limit. You cannot touch my face print. That is an analog of you cannot track. And so basically, there is a direct analog of the online and the offline applications you're talking about.

>> Maneesha Mithal: John?

>> John Verdi: I think that the issue is do not track for facial recognition looks somewhat feasible for photos. You have metadata on photos. You have filename data on photos. You have ways to tag photos that say "Do not use me to generate biometrics, please." It looks like a robot.txt in XFN file, okay? For actual people's faces, you need to be tracked in order to assert your right not to be tracked. There needs to be a generation of a biometric in order to compare it against the do-not-track database. And I think that that becomes less feasible as a satisfactory solution. As to digital photos, I think sure, you've got a number of different standards out there, a number of different ways you can get it implemented technologically for consumers to express their preference. I don't know how I can express my preference on my face short of doing a Mike Tyson.

>> Maneesha Mithal: Yeah. That's not fun at all. [Laughter]

>> Joseph Atick: John, it's not so clear that we agree with your position on that, and there are technical measures that would stop you from taking an identity-tagged and converting it into a face print. I mean, that can be done. You're talking about somebody's picture being picked up in a live video?

>> John Verdi: Sure.

>> Joseph Atick: But in that case, being picked up in live video, the problem is, where is the identity tag coming from?

>> John Verdi: That's my question.

>> Joseph Atick: If it's not identified, it's no identity tag, they don't know who I am. Somebody has to be providing in that chain the identity tag to associate with the face print. If you generate it live, you can generate it live for all you want, but don't store it. And if you store it with the tag of the identity, it must have come from some social-media site or some area where somebody gave the Oracle. Somebody must be sitting on the street saying, "That's John. That's Bob. That's Bill." We want to stop that Oracle from operating.

>> Maneesha Mithal: So, Simon, if you --

>> Joseph Atick: So elaborate.

>> Simon Rice: Just a couple of things I guess on this sort of opt out, really. Again, an opt out, you know, can't really be considered certainly a consent in any meaningful way. And then if there's technical solutions to opt out, well, then, surely there's just as many technical solutions to opt in. So just that sort of distinction, really. A previous point of sort of data retention and minimization, it's really gonna depend back to the original purpose of the processing. What is it? Thinking about crime prevention or something like that, you need to keep it for longer than the session. If it's just for delivering me a coupon, well, do you really need to keep it?

>> Maneesha Mithal: Okay, so, we've talked a lot about notice and choice in the offline world. You walk into a store, and you have a camera. I want to ask Erin. I know that Facebook has implemented facial-recognition technology on your program. And if you could talk a little bit about notice and choice and how you've implemented that and maybe describe how you use facial recognition.

>> Erin Egan: Sure. So, again, as I mentioned, we have some basic principles around our use of it. Number one, it's within the social context, so we are not using facial-recognition technology to identify people who are not known to you. So we are not using it in that way or any of the types of ways we've been talking about. In terms of our controls over how it's used -- well, number one, for tagging, as I think everyone knows, we've talked about today, we allow folks to be tagged in photos. Just like in the old days, you used to write on the bottom of the Polaroid who was in the photo, we do that with tagging. When you're tagged, you will know. You'll receive a notice indicating that you've been tagged in a photo. You can then remove the tag. In terms of Tag Suggest, we only use that with respect to friends. So, again, you've opted in to a relationship with someone because you have chosen to have that person be your friend. When you've opted in to that relationship, we will then use that relationship, and we will suggest one of them to you. So we're not suggesting people you may know or people we think you might like. It's people who you have designated are your friends. And you have control over that tag-suggestion feature. You can opt out of it. You can have it turned off so that it's gone forever. So that's basically how it works. And, again, I think just in thinking about what we've been talking about today, I think so much of it depends on context. And the expectations that users have depend on -- we've talked about this so frequently, and the context in which they're engaging. And with us, again, with this use of facial-recognition technology, we're not using it for commercial purposes, you know, to send you a coupon because of who you are. We're using it to help you identify your friends. It's a suggestion. We're not automatically identifying you. We're just suggesting people who might be in your photos so we can make tagging easier for you. I mean, that's the context. And that's a very different context than some of the others here, but nonetheless, even in that context, there are important principles around notice, around control, around security. We encrypt the tags. We store them in an encrypted forum. So security is very important to us. So, I still think these framework principles apply, but again, I think that when we look at how they should be applied, it should depend on the context and users expectations.

>> Maneesha Mithal: Great. So, I want to weave these two scenarios together a little bit. So, there are scenarios where, let's say, you might walk into SaveMore, and we go through this process that's represented on the slide, and SaveMore partners with another company. It could be an app. It could be an advertiser. Let's say it's an app, and it can broadcast your information that you walked

into SaveMore onto John Doe's friend's Facebook page, "Hey, John Doe is at SaveMore." So it seems that there are current uses of this technology, as we've heard earlier. It seems like most of them are focused on providing opt-in choice. I wanted to see if there are any particular concerns about that kind of scenario, where SaveMore is now providing this information to third parties. I think we've made a lot of this distinction between first party versus third party, and I wonder if it makes a difference here in this scenario. Okay, should I call on someone? Joseph.

>> Joseph Atick: No, the question is I didn't understand what Erin said exactly. At what level is the consent given, and how explicit is the purpose of that consent? So for example, you can say, "Notify me when I appear in a photo." I understand that. So I'm saying every time I appear in somebody's photo, notify me. I've got total control over that. I've got now a social network, lots and lots of my friends. But do I have the right to, even in my own photos, for your system to automatically tag them with my friends' labels without them having explicitly said, "Okay, yes, I will concede, even my friends." Can my friends tag me?

>> Erin Egan: Your friends can tag you in a photo, and then you receive notice. That's right. I mean, you'll receive notice after you've been tagged. But yes, your friends can tag you in a photo.

>> Joseph Atick: Today, my friends tagged me in a photo.

>> Erin Egan: Yeah, just like you can write on the back of a photo.

>> Joseph Atick: Just right on the back of a photo?

>> Erin Egan: Right, exactly.

>> Joseph Atick: But your system, which automatically tags my friends, if my friends wish not to be tagged at all, even though they're my friends, how explicit is their ability to control their friends from tagging them?

>> Erin Egan: Again, I don't know that it is any more explicit than I indicated. I mean, again, you get notice, and you can stop. There's a couple things.

>> Joseph Atick: After the fact?

>> Erin Egan: Yeah. Remember, but you can also prevent the tags -- there's several things to say. One, you can prevent the tags from appearing in your profile, so we have a tag-review feature, right? So if I'm a friend of yours and I don't want you to be able to tag me, or I want to at least control whether or not any tags that you've put me in in any of your photos goes on my page or on my profile, I can set up Tag Review in the first instance so that I can see that. Number two, any photo is only gonna be shared consistent with my settings, so if my setting is set to just share with only me or just share with just friends, then whenever you tag me in a photo, it's only gonna be shared consistent with my own settings. So there's a Tag Review in the first instance. I hope I'm making sense. There's a Tag Review. There's an ability for you to control the audience with whom it is shared. There's also, again, you're gonna receive notice as soon as you are tagged. So those are the controls that we offer. I mean, when we looked at this -- I mean, and, again, when we look at every product, we do take privacy by design very seriously, and we look at it, and that's how we determine that gave adequate notice to the people who were being tagged, gave them control in terms of not having people see photos that they don't want perhaps to be seen on their profile, because they can review them first, and then they can also control the audience. So that's how we manage it.

>> Maneesha Mithal: We have about five minutes left, So I want to give one more scenario, and then I want to let each panelist give their final thoughts. So, the last scenario is let's say we go back to SaveMore, and this time SaveMore appends data from data brokers to the information that they get from this facial-recognition technology. So they might get the fact that this customer is John Doe, but then they use information from data brokers to add what John Doe's prior purchases were at other stores. And I'm wondering if that changes the analysis. I'm gonna call on Pam, because I know that she's thought about these issues before. And are there any other privacy protections that should be in place to address that scenario? How do you explain the idea of data pending to a consumer, and how can you protect in that situation?

>> Pam Dixon: Yeah, data pending is really tough. It's an old problem. It's just a new technology that's doing it. Data pending has been around ever since there's been mailing lists and even probably before that somehow in the Stone Age. But today, the way data pending is working with facial recognition is really amazing. I was at the digital-signage convention, and I literally was watching a display of digital signage that's deployed in an extremely well-known chain. And what it does is that it recognizes the people who are checking out at the cash-register line. As they're checking out, it scrolls their purchase information over their face, and actually right next to it. So they still get the nice face print intact, and it identifies them. And I have to tell you, I think people would really freak out if they knew this was happening. Now, the company sells this for anti-fraud and security purposes, but they don't deny that some customers are "considering using this for marketing purposes." So I think that data pend, when you're adding data to any kind of facial recognition, I think it's really tough, and I think that you have to really increase the level of meaningfulness around privacy protections. There's a lot at stake, because you're forming a mosaic picture of an individual that could have life consequences.

>> Maneesha Mithal: Okay. Can we just go down the line? 30 seconds, each panelist, any final thoughts? I guess the final question I would ask is how can we balance the beneficial uses of facial-recognition and detection technology against privacy concerns and address privacy concerns while allowing beneficial uses of the technology? So let's just go down the line. Joseph.

>> Joseph Atick: Okay. Again, we strongly believe that face recognition is a viable technology, is an important technology in society, and should have a role to play, but it should be part of responsible use. All of the problems that we have heard about today result from the treatment or mistreatment of a face print. I'll drill this back home again. Face print is a biometric. Just like all biometrics, it should be considered as a PII, owned by the identity from which it was generated from, and it should enjoy the protection, one, vested upon it by the status of PII, second, the ownership rights from which it was derived. Everything else could legitimately be derived subject to these principles. Pam?

>> Pam Dixon: I'm interested in no secret collection of consumer information, and I'm interested in meaningful consumer recourse in an era of ubiquitous collection. We've got to tackle those issues.

>> Maneesha Mithal: Erin?

>> Erin Egan: I think as custodians of photos and tags, we have to protect, enforce, and educate consumers about what's there. I think as a user of facial-recognition technology, we have to recognize context, and I think that the principles depend on context. But, again, these principles are notice, control, security -- again, the privacy-by-design principle that we've all been talking about.

>> Maneesha Mithal: John.

>> John Verdi: Infest in masks. [Laughter]

>> Daniel Caron: I don't know if I can beat that. Two quick points. One, although this distinction between are we collecting personal information, are we not collecting personal information might be very interesting as a legal distinction, I think at the end of the day, it's misplaced as a focus point. I think the focus should be on whether we're employing facial detection, facial recognition. It's a question of openness of business practices so that the customers know what they are or are not doing. And secondly, to leave the group off with some optimism, there are certainly success stories out there in terms of the use of facial recognition in balancing that with privacy. We heard from our colleague from Ontario and their discussion with the Ontario Lottery and Gaming Corporation. They sat down. They collaborated. They had a discussion as to how do we balance the use of this technology with important privacy principles. So there is hopefully some optimism going forward.

>> Simon Rice: I think, well, it's just important, really to have a very clear purpose of what you wanted to do with this facial-recognition technology, and then think about how you're gonna explain that to the users. We've already heard today how does a user tell the difference between a camera that's doing all these different types of technologies. So get that notification to data subjects, and, also, consideration of their subject rights, including the access to their data and, also, rights to object to that processing.

>> Daniel Solove: I think that when analyzing this, I always begin with "What's the problem? What problem should we be addressing?" And so I start with there in thinking, "What's the problem with this?" I also think it's important to think about the broader context of facial recognition from all sorts of types of data, such as GPS and other data that could track our location or that could identify us in public and think more broadly, 'cause we could solve one problem, but then there could be a whole host of other related things that could do the same things or the functional equivalents of facial-recognition technology. So I think we need to think about substantively what are the problems we want to address and then start focusing in on how do we allow the benefits of these technologies, but at the same time address those particular problems that they're causing. But think broader than just facial-recognition technology, which Is a major issue, but there's a lot of other related technologies that could also cause some of the very same problems.

>> Maneesha Mithal: Okay. Thank you. And thank you to all of our panelists. This has been a great panel. Thank you so much. [Applause] Okay, and then finally, we have closing remarks from the deputy director of the Bureau of Consumer Protection, Jessica Rich.

>> Jessica Rich: Hello. Okay. So, good afternoon. The main thing I want to do with my closing remarks is thank everybody. This has been an incredibly productive discussion. Fascinating, too. And I want to also commend all of you. This is such a crowded room for the end of the day. It's quite impressive. Most people stayed for the whole thing. I also want to sum up what I think were the main themes, which I think everyone will recognize today, and it was many of the things that these panelists just said. I think one key theme today was consumer awareness, obviously. The consumers realize when facial-recognition technologies are being used, do they understand the potential consequences of having their images captured and potentially stored for long periods of time and used for other purposes? I think there was some consensus that consumers should receive some form of notice when these technologies are used. The finer questions of how this notice should be provided, how much detail to include, and who should deliver it prompted some debate. This is clearly an area for future work. As for consumer understanding of the potential consequences of this technology, we heard from a lot of panelists about the need to educate the public, and we strongly agree about that. This workshop was to start that process. Understanding

that technologies are being used, how they could be used, how they'll shape consumer experiences as we move forward is critical given that these technologies are very likely to be greatly expanded and used more in the future. A second theme that came out of the discussion and actually dominated the discussion was how much control consumers should have over information that's collected about themselves through these technologies. Many panelists said that consumers should have the ability to choose whether their images are captured by facial-detection or recognition systems in public spaces. Some also said consumers should have the right to see what information is collected about them. And as we heard, though, exercising choice about how your image is used can be extremely challenging, especially when the images are captured in a public place, such as a supermarket. There was a fair amount of agreement that the level of control that's needed does depend on the number of factors, such as the extents to which a person's image can be personally identified, whether it is gonna be linked to other personal information, how the data is used, the context -- I kept hearing the word "context" -- and whether the data will be retained or transferred to third parties. All of those factors are really gonna make a difference in terms of what protections are needed. Finally, a third theme we heard is the importance of incorporating strong privacy protections into both the development and the operation of these technologies. We heard that some companies have chosen to develop their products in a manner that makes them more privacy protected, such as by not retaining images, consumers, past the initial use. We also heard about some search engines and social networks and photo-sharing sites that control vast databases and that they could implement measures that could limit the mass capture of images or detect and limit automated scanning of images by web crawlers. We also heard there may be places where facial detection and recognition software shouldn't be used at all, like bathrooms and doctors' offices and aisles of the store where sensitive data is sold. The FTC, as you know, encourages all companies to incorporate privacy by design in these technologies, as well as others, to build their technologies with privacy in mind, to think of ways to minimize data collection and retention. This is still a young field, so it's really the right time to consider privacy as the technologies and the business models continue to develop. So, where do we go from here? First, we recognize that not everyone could be on the panel, but there's a lot of very knowledgeable people about these technologies. So we are keeping the topic open for comment until January 31, so if you have additional thoughts and comments, articles, other materials to send, please send them on to facefacts@ftc.gov, our page. Second, as many of you know, last year, we issued a preliminary

report, staff report, proposing a framework for safeguarding consumer data in a way that would protect consumers, but also allow business models to thrive and develop and everyone to still get the benefits of all these new technologies. We expect to issue a final report soon. Is there an expression, "real soon," in -- [Laughter] Yeah, real soon. Ed Felton said that on a panel yesterday, and everyone thought that was really funny -- "real soon." Well, in the coming months, we do promise, and we're gonna consider what we learned here today as we developed that report. To the extent needed, there may be an additional report on this particular workshop or other follow-up. I think there will be other follow-up. Obviously, we're gonna continue to monitor this marketplace as it develops and examine whether the privacy issues we've discussed today are being incorporated into the technologies. So, and finally closing, I'd like to thank some of the FTC folks by name who worked on this great event -- Manas Mohapatra. I don't know where he went. Over there. Amanda Koulousias, who's over there, Jessica Lyon, Laureen Kapin there, Cheryl Thomas were the key FTC people who put this together. And I'd also like to thank Carey Galoula, Wayne Abramovich, Christopher Huntsik, T.J. Peeler, Andrew Schlossberg, and Leah Potash, who also helped and did outstanding work. You see what it takes to put together an FTC workshop? It seems so simple when you come for the day. So, anyway, once again, thank you for coming, thank you for watching, and thank you for your incredibly valuable contributions today. [Applause]

>> Male Speaker: Good job.

>> Jessica Rich: Yeah, thanks.