>> 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

>> 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-iusw 4.(he)-d(ade)-1( )d(, w)2(ha)-1(r)-1, sti of

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

>> 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

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.

>> 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

>> Laureen Kapin: It's aggregated.

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

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 th

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 wi6

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.

>> 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,

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

>> 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

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

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

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:

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

I don't know the answer to that. I think it involves a lot of study about how people decide and then how best

>> 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 agade1(f)3(i)fnatriu]TJ 0.001 Tc -

>> 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 relation1(l)s,c(d, you w)2(i)-2(l)-2(l)-2( )-2(l)-1(y or)-

>> 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 jush -2(y)]TJ TeehT oring p11(a)4(p)1(u)8(e)-1(,)-1(s)4((e)-1(t(e)-1(1(put)-2(hT)-(m)8

>> 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

>> 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

s

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.