>> Manas Mohapatra: We're gonna get started for the second part of the day. Before we get into the substance, let me just reiterate some housekeeping notes that we already heard earlier today. As most of you have discovered, anyone that goes outside the building without an FTC badge, when you come back in, you're gonna have to go through the entire security process again, so just take that into account.

>> Male Speaker: [Inaudible]

>> Manas Mohapatra: [Laughs] Sorry about that. In the event of a fire or evacuation of the building, please leave the building in an orderly fashion. Once outside the building, you need to orient yourself to New Jersey Avenue, which is across the street this way. Across from the FTC is the Georgetown Law School. Look to the right-

detection technology -- uses that until recently seemed the stuff of a distant future or a galaxy far, far away. But here and now, advertisers are using facial-detection technology to identify the age and gender of a face exposed to their ad space and targeting their marketing to the demographics identified. A 20-year-old woman might be shown an ad for perfume, a 30-year-old man an ad for shaving cream. We also heard about a mobile application that checks out who's at a bar so users can scope out the scene before they even arrive -- a new twist on see and be seen. Back in my day, you had to do a lap around the bar before committing to the optimal barstool. [Laughter] And now you can do it from your home. These advertisements and apps rely on facial detection, not facial recognition. While they gather general traits, often in aggregate, they don't identify specific individuals. But as the chairman's remarked this morning, if not now, then soon we will be able to put a name to a face. For me, this subject brings to mind one of my favorite songs. It's a song of The Beatles. And for those of you who are under 40, just to let you know, The Beatles were a rock group. [Laughter] They had a hit or two in the 1960s. The song is "I've Just Seen a Face." It's a classic about love at first sight. It all happens at the first glimpse. Paul McCartney tells us nothing about the object of his affections, not even her name, probably because he doesn't know it. I can't help but wonder if this song might have turned out differently if facial-recognition technology had been around in 1965. What if, when McCartney saw this face, he had instant access to more concrete information about its owner, like her name, her date of birth, or place of work, her e-mail address, online purchasing history, or other personal information? Now, let's assume that, like me, she wouldn't have minded if a young Paul McCartney had invaded her privacy just a little bit. [Laughter] But what if she did? Or what if, instead of one of the Fab Four accessing her information, it was an acquaintance that she wanted to avoid or an insurer deciding she was too high of a risk to cover based on a photo of her skydiving or a potential employer judging her character based on a picture someone put online from that party freshman year? Or what if the technology confused her for another person? We saw this morning how technology doesn't even get the gender of the person that it's looking at right. [Laughter] And, Brian, if you're back from lunch, so sorry. [Laughter] It's scenarios like this that we must bear in mind as we both guide and react to how these technologies change the way we buy, sell, and live. This afternoon, we'll talk about what we can already use facial-recognition technology to do, what we can expect in the

companies already using facial-recognition technology, like Facebook, Google, and face.com. We'll hear how Facebook and Google are using this technology to make it easier to tag photos of friends and families. We'll hear how face.com, which is a start-up in Tel Aviv, how it's using app development -- I'm sorry, it's giving app developers the capability to use facial-recognition technology in their own apps. And we're gonna hear from Chris Conley from the ACLU of Northern California, who will share his perspective of facial-recognition technology from the viewpoint of an advocate for consumer privacy. Along with learning about the commercial uses of facial-recognition technology, we'll also hear about a groundbreaking study to determine exactly how far the technology has already progressed. Can it identify previously unidentified photos? Even a bit more surreal, can it match students walking on a college campus to their social-networking profiles? We're pleased to be joined today by Alessandro Acquisti, a professor of information technology and public policy. He and his team at Carnegie Mellon tested whether an individual's partial Social Security number could be guessed accurately using only facial recognition and publicly available information. The results of this study were surprising, and we look forward to being surprised again by Professor Acquisti today. To conclude our workshop, the last panel will discuss the policy implications of the increasing commercial use of facial detection and recognition technologies and address two issues. First, what protections for consumers are currently in place? And, second, what protections should be in place? I'm gonna be particularly interested in the part of the discussion of that last panel about mobile applications. If a user takes a photo and tags friends in it with an app using facial-recognition technology, will the friends who are tagged be notified? Will they have to consent to the use of their photo or the use of facial recognition? And if so, how will we at the FTC and how will other regulators enforce these privacy provisions? Now, we're honored that our fellow privacy regulators from Canada and the United Kingdom have joined us today, both as panelists and attendees. First, I'd like to thank my friend and colleague, Jennifer Stoddart, Canada's privacy commissioner, for being here. Dan Caron from her office will also be on a panel later this afternoon, and we're delighted that Dan is back at the FTC. He had spent several months with us back in 2009 as part of the FTC's international-fellowship program. Also from Canada, we're pleased that Fred Carter from the Ontario privacy commissioner's office is here with us today. Fred, I think, was one of the panelists earlier this morning. And from the United Kingdom, Simon Rice from the information commissioner's office is joining us, and we'll hear from him this afternoon. We're delighted, as the chairman mentioned

this morning, to have representatives from a number of organizations in the privacy-advocacy consumer, academics, and from industry. We value all of your input as we strive to protect consumers navigating the marketplace. And last, but very much not least, I want to congratulate the FTC staff who worked tirelessly in putting this workshop together. We and myself in particular are very, very grateful for your efforts. So, what better way to end my little afternoon opening remarks than to return to Paul McCartney? When he saw the face that he thought was "just the girl for me," he wanted all the world to see that we've met. In 1965, he did that by writing a song. Today, he could have just tagged a photo in Facebook. Tomorrow, who knows? I think we'll all have a better idea of what the future holds after hearing from our panels this afternoon, so thank you very much for being here. [Applause]

>> Manas Mohapatra: I think we're gonna get started straight through with our third panel of the day.

>> Amanda Koulousias: Good afternoon, everyone, and thank you, again, for joining us for our afternoon panels. My name is Amanda Koulousias, and this is Jessica Lyon, and we are both staff attorneys in the Federal Trade Commission's Division of Privacy and Identity Protection, and we will be moderating this first panel of the afternoon. Before we jump into the substance of the panel, I just want to go over a couple of administrative details. We'll begin the panel with some of our panelists giving presentations, and after they have presented, we will have a facilitator discussion exploring some of the issues raised in the presentations. For those of you here in person, there are question cards in the folders that you should have received when you walked in. If you have a question that you'd like to ask one of the panelists, you can fill out the card, and there will be FTC staff circulating. If you'll just raise your hand, they'll come and get the card and bring it up to the moderators, and we will try to incorporate as many questions as we can into the discussion. If you're watching on the webcast and would like to submit a question to our panelists, you can also e-mail it to facefacts@ftc.gov, and somebody will be monitoring that e-mail address and bringing the questions, as well, to the moderators. It's definitely possible that we won't get to everybody's questions, but we'll try to incorporate as many as possible. Moving into this panel, this morning we heard from a variety of panelists about the use of facial-detection technology, where consumers are not being individually identified, but their demographic characteristics or emotions are being

ascertained. On this panel, we will be taking it a step further and discussing facial-recognition technology that can and does identify individual consumers. We'll be hearing from both Google and face.com about how they are currently implementing this technology in their products and services. And as Commissioner Brill mentioned, we'll also be hearing about the recent study out of Carnegie Mellon that was using facial recognition and its resulting policy implications. And then finally, during our discussion, we'll be discussing the potential privacy concerns that may arise from both these current uses, as wehsa(l)-2(l)-8Tr finallyo -0.001 Tw T* [(f)4(r)-oal bese5 Td [(f)3(tio)2(n)7(s)

And as we've said publicly, we don't want to deploy this technology until we feel like it's ready and that we have the privacy protections in place. To highlight the privacy principles behind the way that we think about this, I'd like to just go through them very quickly. These are the intersection of technology and privacy, and these are what sort of guide us in our deployment in building of products. First, we want to make sure always above all that we are building valuable products that users would like and that they find useful. Of course, those are built with strong privacy standards and practices in place. And there's got to be transparency around how the products work, meaningful, relevant choices that give users control and security. At the start of the talk, we talked

but you may have heard of it. It's from the Ice Cream Sandwich operating system, which is the newest operating system from Android, and it's available on certain Android devices now. What you're looking at is a screen shot of a feature called Face Unlock. This is the low-security entry point for users that essentially most likely will have no security on their phones. As you know, a lot of users just simply have their phone sort of swiped to unlock, have nothing there. And this is a good entry point to help someone who may not be ready to start typing in an onerous password or deal with that in some way, and this gives them something more than what would just be the default on the telephone. The way that this would work is the user goes into the settings, takes a picture of herself. This picture is then stored on the phone as the key image. And then when the phone is locked, the user would like to unlock it, she essentially performs the same action. It takes another image and compares the area that is detected to be her face, recognizes that, and compares it between the key image. If there's a match, the phone is unlocked. If it's not a match, it's not. The next example that I'd like to talk about is another example of facial recognition, and this screen shot is from Google's Picasa desktop client. This, in case you're not familiar with it, is Google's desktop photo-management and editing software. And what you're looking at here is actually a screen shot from my Picasa. That is the face album for me. And what you see is a bunch of photos of me, as well as a bunch of photos that Picasa thinks correctly are me that I have not yet accepted that are there. You see the check mark and the "X" underneath those. With Picasa desktop client, we allow users to locally manage face models on their computer. These models can then be used in turn by the user to help to organize their photos. Obviously, we're in a time when the proliferation of digital cameras, they're everywhere. People are taking photos. They're getting CDs and photos from friends, e-mailed photos. This is way for a user who wants to organize these on his computer to put them all together, organize them by faces, see whose image albums, kind of quickly go through them. Also to, of course, tag the people in the photos if they'd like to. The next example that I'd like to talk about, the final example of what's possible now, is this feature called Find My Face in Google+. As I explained at the beginning of my comments, we like to build these products at Google with the privacy principles firmly in mind. A marquee example of how we've done that

course, can also be deleted individually if the user would like to. Since the feature just launched today, I'm sure that none of you had a chance to tinker, but I hope that through the description, you can see the thought that went into this and the way that privacy has been baked in from the beginning with this feature. And the second part of the title of today's talk is "What Does the Future Hold?" And I'd like to just briefly finish my remarks with a couple of examples of ways that computer-vision technology, pattern recognition, facial detection, facial recognition might be used in some interesting ways coming down the pike. Obviously, the engineers that work on these offer a lot of promise, and this type of thing could make great contributions. Two specific areas, perhaps extensions of some existing projects that are already done, could be things that come around. As Chairman Leibowitz recognized this morning, child exploitation is a serious problem. In 2008, Google engineers teamed up with the National Center for Missing and Exploited Children and help to develop pattern-recognition technology that could be used to run across large collections of

find out who it is?" Or, "Here is, you know, a date, you know, from last night. Who is she?" Right? Our answer to all of these, by the way, is the same. We can't do that. Right? We can't do that. And the reason we can't do that is because we have rigged privacy from day one so it's limited to very specific context. And that's what I want to share with you. All right, so, face detection.

we are that this is a face in a photo. And then you can see the results. We're 82% in that case that this is Gil Hirsch. Then a number of my friends are there, as well, so I can put those -- one of them, actually, is a little bit similar to me. He's not me though. All right, how it works, very quickly. Face detection -- easy. You send a URL, and we'll spit back the answer. We don't provide you with any more information, aside from the mental data that we extracted. You won't get anything to hold, but we'll give you that information. With face recognition, we have to provide is reference photos of the people that you were looking for. So you can't ask, you know, "Here's a photo. Let me know who it is." You have to provide both, all right? "Here's a set of photos. Here's the gallery," right? "Here's the photo. Please do your comparison and let us know if one of those was found there." Nice work, Greg. So, I want to talk about privacy. This is about privacy, so... Since day one, we asked ourselves how do we avoid the one use case that everybody fears, which is to de-anonymize people. So, the first thing we said, "You don't know everything and everyone." That is, we're not going to hold a huge database of photos for you. We're not gonna hold a huge database of people for you to look for. You're gonna have to know both. So the input into our system is both the photos and the people that you want to have identified, and that will give you back the answer. So, in fact, you can never identify people you do not know. That's our mantra, right, is this one thing that we wanted To make sure that doesn't happen. And in addition to that, we've limited the scale, so you can only do that up to a certain amount. You can't flood our system with data. You can only set a certain scale. So the gallery is only that big. And within social networks, we have also added a concept of friends, so if somebody is a friend, we'll add that additional layer where we try to validate that. "Am I a friend of Greg before I can even ask for Greg to be identified?" Right, so I cannot identify anyone who is not my friend. But, again, keep in mind that we are operating a service. This is the things that we have applp

first thing to appear on the screen is on the top-left, then the top-middle, top-right, and then we go down following these arrows, okay? So, as I said, we lost all the dynamics here, sadly. I get an anonymous face, in the street or online. I find the matching face. Facebook's just an example. LinkedIn, organizational rosters --

good photos of themselves and using their real names. Therefore, what does privacy even mean in this kind of future? So, I was asked to discuss is this worrisome? If so, what are the scenarios I should be worried? Well, technologies such as face recognition can be used, as many other technologies, for good and for bad. So, you have at the center in the street that you recognize as a person that you met at a party. Good purpose, right? Especially a conferences such as this. We all

show each single person. And you know what? In some years, with sufficient computational power, you cannot just identify these three people and all of them, all the rest, but, in fact, in real time see whether they are connected or not in LinkedIn or Facebook, by what degree of separation they are connected. In real time, you can overlay the online connection to their physical disposition on a place. It can be used for good -- avoid criminal or terrorist attack. It can be used as a way to control, also, your right of free speech or be anonymous as you go through a political event. Now, this, of course, is not happening yet. Currently, we cannot do face recognition of everyone, everywhere, all the time. There are a number of challenges -- how many faces, partial images, are really available to you Versus to big corporations versus the government. If we start using databases of your hundreds of millions of images rather than hundreds of thousands, which is what we did, well, you start having big problems in terms of accuracy and especially false positives. I used to joke about the fact that as you start working with hundreds of thousands of images, you realize that you are not a unique and beautiful snowflake. [Laughter] There are many people who look like you. And face recognizers, a problem with this, underperform humans. We used comparative subjects. Our students, our subjects, were sitting in front of us. In the street, you cannot really stop people and ask them, "Hey, can I recognize you? I'm a stranger. But, you know, stop for three seconds while I take your photo." Computational costs. The bigger database, the more computations you have to do, and even cloud-computing costs start being quite expensive. However, current technological and business threads do suggest that all these limitations are not systemic. They will fade over time. So consider how many images are now existing compared to what they were 10 years ago. Imagine what will be 10 years from now. In 2000, this extrapolation based on a paper, publishing site, academic journal would not be your photo shot worldwide. Unless you are a celebrity, your photo didn't going online. Only a miniscule percentage of this 100 million went online. In 2010, only on Facebook, only single 2.5 billion photos uploaded online. So

names, and your name is also public by default. If you want to use your face for your primary photo, of course you're free not to do so. But we wanted to estimate how many people do use their faces, and Ralph just passed me the numbers a couple of days ago. We randomly sampled out of the publicly available Facebook directory, without even needing to log in Facebook, about 2,000 profiles. About 49% of them had a unique face. About 60% of them had at least one face. So focusing on those with a unique face were arguably likely that's really the person. And knowing that 90% on average have real first and last names, out of 800-plus million users, these suggest about 330 million unique-identified faces accessible through their public directory. Accuracy -- I will go quickly here, because, as mentioned this morning, also, by Dr. Phillips, the accuracy improves by about an order of magnitude every four or five years. So comparing 1997 to 2010, dramatic increase in accuracy. And, in fact, researchers are very well-aware of all these problems wipron

antenna. So this contact lens can connect through some other server, through Wi-Fi, and has a LED to project information which could come through the antenna. It has not been tested on humans yet. That's not a very airy, human eye. It's a rabbit eye. But the rabbit did survive. [Laughter] So 5, 10 years out, you can imagine what sounded crazy to Ralph and me just three months ago, which is your eyes looking at people and highlighting information in real time. Plus, there are these business trends. I will go quickly here, because we have many representatives of the companies who are involved in face recognition, and we have already seen how hot and stimulating the business environment is in this area. So the short is, currently, what protects us -- if you feel that we have to be protected. I would grant you that we can debate about this. If you feel that we should be protected from the kind of future that I alight, where anyone could look at you and predict sensitive information about you, what protects us are mostly false positives, so the scale of the problem, and regulatory self-constraints. So the issue is, for how much longer this will act as protection? Let me quote and say I didn't -- here is completely my fault I couldn't put -- the slides, I gave them too late, because we were crunching numbers. We were on supercomputers, and they only produce the results this month. I'm kidding, I'm kidding. The numbers are not -- they didn't need supercomputers. They simply were back-of-the-envelope estimates, extrapolations that we did. Think about this. Currently, we are protected by self-regulation in the sense that, for instance, "Gee, very eloquently notice how protective of the usage of facial information they are. Now, compare now to 10 years ago, how much information about you was available to others, to corporations, for instance, years ago. You would be surprised if you could go back in time and think about what we have now. So extrapolating years out, what will be more accepting in terms of information known about us. And now consider the technology. Today, with the cloud-computing cluster we were using, which costs $2 an hour, we were able to compare a pair of images in 0.0000108 seconds. If you wanted to do what we did, rather than how we did it, which was just hundreds of thousands of individuals, if you wanted to do it nationwide, say 300 million people, we would never be able to do it in real time. It would take four hours for each face that we tried to match -- four hours. Impossible. Imagine 10 years out, 2021, the population of the United States will be about estimated to be 337 million. Consider just the population which is 14 years and older. Let's assume there is Moore's Law, and therefore a certain improvement in cloud-computing power over the time. Let's assume simply the only pre-massaging of data we do is that we split male images from female images. 10 years from now, we could compare one random shot taken here to

everyone in the U.S. in five minutes at $2 an hour. If you want to spend more or if you assume that competition will bring the cost of cloud computing down, you could spend $60 an hour, and this comparison can be done in 10 seconds. My point is that we ca

case. For instance, obviously, if the user doesn't want to opt in, they don't have to. But With the example it would look at things, for instance, like a circling relationship or a bidirectional, circling relationship, or perhaps if you had e-mailed somebody in Gmail and had, you know, a series of conversations with them in that, it might use that information, as well, so those kind of vectors. And, obviously, as people start to use the feature and if, for instance, we start to hear from users that this is something that would be very valuable, obviously, we're continuing to develop it. And, you know, we always look for feedback and are interested in hearing those things, so we definitely welcome any comments.

>> Amanda Koulousias: So, then, exactly who right now would be suggested to users? I mean, I know you said, you know, social, but can you be a little bit more specific?

>> Benjamin Petrosky: So, the way that it's described to the users is people that you know or that we think you know, and so it's essentially starting I think with looking at, like, the circling relationships and then bidding out of that. There's a number of different types of affinities. For instance, if you are posting frequently and plus mentioning somebody, if you were continually sharing albums with somebody, if you're always sort of plus-oneing somebody's content, those are the kind of things that could play into this factor over time as the future develops.

>> Amanda Koulousias: So, then, would that go both ways? So, for example, if I am frequently sharing albums with a particular person, but they are not necessarily sharing albums with me, you know, maybe they have a different view of our relationship than I do. [Laughter] So would they be suggested to me in that instance?

>> Benjamin Petrosky: I know, and that's exactly the kind of work that's going into the development, because that's one of the benefits, I think, of doing a slightly dynamic model is that it doesn't have to necessarily be a bidirectional sort of if I get suggested to you, you would be suggested to me, and it would allow for allowances to that type of thing. If you see somebody who's just, you know, aggressively plus-mentioning somebody and is never being responded to, that might be a signal that that person isn't actually connected to that person.

>> Amanda Koulousias: So is the somewhat evolving nature of this explained to consumers on the Google+?

>> Benjamin Petrosky: I think that the way that we tried to describe this is making it clear in the sense that it is not just limited to circles, for example. The future, obviously, as I mentioned, is a complete opt in. So if it's something that there's any concern about or any worry, the users don't need to engage with it, but using the description of people that you know, and that's the goal that we have, of starting with a small group of people who we have strong confidence that there's a relationship that you would, you know, most likely want to be shared with there and then sort of developing that as time continues.

>> Amanda Koulousias: Okay. You know, you just mentioned that users don't have to opt in to it if they don't want to. A couple of our audience members have actually posed the question, if a user chooses not to opt in to this, is there some other easy way for them to scan the service to determine all of the photos that they themselves are tagged in in order to remove those tags?

>> Benjamin Petrosky: Yeah, absolutely. If you go into the photos tab of Google+, there's a "photos of me" section, and you can click that, and that will link to photos that are linked to your profile. And, of course, you can just click on those and remove any tags that you'd want from there. And just also to mention, I don't know if people -- I see a few laptops around here. I don't know if people have tried to look for this. But as with several of our features, it's a rollout over a course of time, so I'm not aware that it will necessarily be available on everybody's account today. So that, should be, I think by early of next week should be available to all accounts.

>> Amanda Koulousias: Okay, great. And, Ben, not to pick on you, but I know we have some questions for Gil in a second. But, you know, I think one more question about this Find My Face feature, actually, a couple of the audience members and some people who are watching on the webcast have raised this. Are there safeguards that exist that would prevent somebody from using somebody else's face and then being able to use Find My Face to find all of the photos of that person, as opposed to themselves? So, for example, if I uploaded a photo of Jessica?

>> Benjamin Petrosky: Right. So, if the model requires that the faces be tagged to your profile, so assuming that you have, you know, a number of photographs that are tagged to yourself and you, you know, tag the president in a photo as yourself, or you tag a piece of a tree or something, obviously, the statistical algorithms are gonna look at those and are going to have more heavily weight to the information from the photos that are sort of the group there.

>> Amanda Koulousias: Okay.

>> Benjamin Petrosky: And thank you for the feedback. This is great. And, of course, we always, as I mentioned before, are interested in hearing and do appreciate any of this kind of feedback, so we would welcome it. Thank you.

>> Jessica Lyon: Excellent. Thank you. So, we have an audience question for Gil, actually. So, the member of our audience was wondering if a consumer requests that you delete all images of him or her, do you honor that request, and how does that process work?

>> Gil Hirsch: Oh, absolutely. So, there's a way to opt out, again, out of an existing social network. The one feature we do not support currently, because it's technologically not possible, is for you to

>> Gil Hirsch: No need for photos. You all know Facebook Connect, just as an example, right? So, you click a Facebook Connect, and your I.D. on Facebook is the only information that it will keep. It's like a blacklist of people that if these people are being asked for, they're ruled out automatically.

>> Amanda Koulousias: And is there a way that somebody could delete any information face.com might have about them if not connected in any way to one of the social-networking services?

>> Gil Hirsch: So, we haven't found a reasonable way to do that yet. We do, however, require that if you're using our system, not through an existing ideaf 12 0 0 12 65.9G 12 65.9ly. 0 12 63tem, not2(f)3(,)4(t)-

? 0 Tw T* [(m)8(i)12.7Tj EMC /P <</MCID 3 >>BDC -31 ( )

color. And now you're using all this information and making decisions about the person based not on what your gut feeling is telling you, but on this machine, on this algorithm. In a way, incredibly exciting from a side. Also incredibly creepy from another side.

>> Benjamin Petrosky: I just had one point as I was thinking through it. It occurred to me in responding to the question about the person who had asked about tagging faces that were not your own in your model, and I think that what the questioner might have been getting at was the idea of instead of having a collection of your own faces of just simply using the profile to tag, for instance, you see a picture of somebody in a club or on a train, and you take a single picture of them, and then you create this profile to use that. The way that the system has been architected with the necessary social connections in place makes that impossible, so you're not going to be able to just -- a

incredible amount of data already out there, all right? There's a lot of public information already out there. Alessandro has pointed that out. I think one more area where we can look at to add control or privacy or at least think about those are the uses, okay? So it's another approach to how we deal with data versus not only "Is that data there? Is that data not there?" 'Cause in many situations, it's already there. But, rather, what are proper uses, what are not proper uses, you know, even without any specific consent? Because, again, it can always be abused. So what is that abuse line? How do you not cross it, you know? That will be very interesting.

>> Amanda Koulousias: Okay, thanks. Ben?

>> Benjamin Petrosky: I just want to say thank you again, and we look forward to continued discussion on this.

>> Gil Hirsch: Good one. [Laughter]

>> Chris Conley: Sure, make me look bad. [Laughter] So, I will echo that I think notice and control are necessary, but not sufficient. And I think what Gil touched on is something important, that it's not just what information is collected. It's also how long is that information stored, in what format. Is it reverse-engineerable? You know, are you retaining whole pictures or just the face prints or, you know, computational values you need to identify it later? It is certainly about use -- who can use the information, how can it be used, how often can it be used. Face's idea of throttling --

control you're giving and you've reached that, there have to be consequences. And, as well, there have to be protections in the back end so that you can't be forced to breach those. One of our big concerns is with electronic-communications privacy law. And if the law says that someone can come in without a search warrant and just demand information from you and you have to comply, as a company, you can't do anything. And so we want to see stronger laws so that as this information is protected on the front end, you make your promises, you don't have to say, "Well, except if we're forced to disclose on the back end," because we don't have the security, we don't have the privacy law that we need to protect that. So that's what we would like to see.

>> Male Speaker: Hear hear.

>> Jessica Lyon: Thank you, all, for your thoughts and for coming here today and presenting to us. I think we all enjoyed it and learned a lot. We're going to take a short break right now and return at 3:00 P.M. for the final panel of the day, which will address the broader policy implications of both facial detection and facial-recognition technology. So, again, please return to the room by 3:00 P.M. thank you. [Applause]