>> Manas Mohapatra: All right, good morning, everyone. My name is Manas Mohapatra, and I'm an attorney here at the FTC. And I have the pleasure of serving as the moderator for this panel. This panel is going to discuss facial detection technology, which -- it was alluded to earlier this morning -- focuses on using someone's facial characteristics to determine certain general characteristics about them, such as their age range and gender, but isn't focused on identifying who that person actually is. Today, we're going to be hearing about different ways that this technology is being implemented and explore what the privacy and policy concerns regarding such use are and how best to address them. Before we get started in the substantive discussion, I'd l

ads that are being displayed -- that is all that you would see. The rest of this demo is kind of taking you kind of behind the scenes. So, I am going to get in front of this sensor here. And you see that that box means that the sensor has detected a face. And because it is blue, that means that it is a male face. So, how do we do this? First of all, the sensor has to detect that it is a face. And I need to turn, actually. So, this is just the ad display. What I'm gonna do -- Now the targeting is on. So you will see that, since I'm a male, they are showing a BMW ad to me. What this does is that the sensor first looks to find that it's a face. And it looks for eye sockets -- not the eyes. We don't know kind of the color of their eyes or anything like that, but it looks for eye sockets. Once it's determined that you have two eye sockets, that it's a face, then it looks to other things. It looks to the ears. So, for example, if two ears are showing, there's an 85% chance that that person is a male, as opposed to a female. There are females that have their ears showing, but the software and the algorithms just go down different decision trees. We also look at the nose and the lips and the cheekbones. And so there are mathematical differences between male and female cheekbones, and there are mathematical differences based upon age. So, for example, let me show you that if I put one hand over my eye, that two eye sockets have not been detected ,so it's not going to detect a face. And then once that's removed, there is a face again. We don't track. We don't record information. If I look away and then I look back again, it will register that as two different viewers or two different individuals. And you'll see kind of a rotating down here. It also shows kind of the age range. So, here is the age. So, half time, it detected me as a young adult. Half the time, it detected me as an adult. So, again, I'm 39, so I would fall in the adult category. The young adult is 18 -35. So, you know, sometimes the software was a little off and made me look a little younger than I am. So, if there are any female volunteers that want to -- just to see. Do you want to just come up real quickly just so we can show how that works? You just want to stand in front of the sensor here. I'll get out of the way. So, there it -- detects that it's a face. It actually shows that it's a male face. [Laughter] So, there we go. Okay, let me look again. Okay, so for -- it's, you know, the lighting, whatever else. You people have asked about accuracy, so we have -- For gender, we have usually about like kind of a 94% accuracy for age range. We have about a 90% or so accuracy rate. Thank you. So, anyway -- [Laughs] So, that is the -- you know, with the lighting and all that. Thank you for volunteering. [Applause] And so I think, Manas, that's the denouement

>> Manas Mohapatra: Great. Just a few follow-up questions. You had mentioned, in terms of the prevalence of this technology, that this was in the low single percentages. Can you just give some raw numbers? Is that over 100,000 signs, you would think, in the U.S. right now that have it or less?

>> Brian Huseman: So, as far as numbers and kind of market share, we don't have that. But what we, you know, do know is that in 2011 there were probably about one million faces that were detected by our AIM Suite software. So, that's the number that we have.

>> Manas Mohapatra: Great. And just one other question that was alluded to in the earlier panel was that some of these systems can detect ethnicity, and I was just wondering if the AIM Suite can detect ethnicity.

>> Brian Huseman: No, we do not detect ethnicity. We decided we did not even want to try to detect ethnicity. There are mathematical differences between different racial categories -- you know, bone structure and those things. So, the algorithms kind of take those into account, but there is no detection of ethnicity at all.

>> Manas Mohapatra: Okay, great. Thank you very much. Thank you. Our next presenter is Harley Geiger. He is a policy counsel at the Center for Democracy and Technology. His work at CDT is focused on consumer privacy, health information technology, and national security. He's worked extensively on the issue of out-of-home behavioral advertising, serving as a member of the Standards Committee of the Digital Signage Federation, where he led the trade associations initiative to adopt digital signage privacy standards, which cover facial recognition. So, Harley.

consumer privacy legislation that is comprehensive and that covers numerous information categories. However, that legislation will also have an exception -- properly so -- for publicly available information. And there's a strong argument to make that if you're walking around without a mask, you're making your facial features publicly available. And prohibiting individuals from taking a picture of publicly available information could raise some pretty serious free expression and First Amendment concerns. So, instead, we think that the baseline consumer privacy legislation should support a safe harbor that is based on codes of conduct for industry that are voluntary, but that should offer, as companies, some tangible incentives such as a reduced form of liability if they are to adhere to them. And any code of conduct like that must be enforceable. So, we also recommend that the Federal Trade Commission and state A.G.s oversee the compliance with those codes of conduct. And this approach is more or less endorsed in the Department of Commerce's green paper on privacy. So, the industry already has a head start on codes of conduct -- the digital signage industry, at least. So, POPAI, the Point of Purchase Association International, and the Digital Signage Federation both have codes of conduct that do cover facial recognition and facial detection. And they did this in the absence of major scandal or significant government pressure, which is really quite different from the way things went with the online behavioral advertising industry. So, this is very encouraging. So, the digital signage privacy standards with the Digital Signage Federation -- they apply. For full disclosure, as Manas had mentioned, CD1(o7i2( )]TJ ()-1

faial [(t)-campol S-1(he)-1(a)-1ao,w [s.gau

policy available on the Website because if you walk into a Wal-Mart, for example, you don't know

there? Is it just the fact that not many signs using this currently, or could industry be doing a better job in terms of providing notice?

>> Harley Geiger: So, industry could be doing a better job, but it depends on the company. And some companies I know are compliant with the guidelines, and they do provide that notice. However, I have seen in press reports companies literally declining to point out which signs actually have facial detection or facial recognition and -- quote -- say that they don't want their customers to feel uncomfortable." But my argument is that the secrecy will sensationalize the issue and will actually lead to the consumers feeling much more uncomfortable. So, the industry could be doing a better job, but, you know, some companies are doing a fine job.

>> Manas Mohapatra: All right. And one other follow-up question -- if I understood you right, for the lowest level of privacy impact for technology that is using facial detection, the idea is that you can opt out by not entering the premises of a place that has these signs. Is that right?

>> Harley Geiger: Right.

>> Manas Mohapatra: So, do you have any thoughts about, should this technology not be implemented in particular areas -- for example, you know, healthcare facilities 00 so that people don't have to make that kind of choice?

>> Harley Geiger: Yes, actually. So, healthcare facilities, locker rooms, bathrooms, a lot of places that people must go to and really have little choice in going to. You could argue that a supermarket qualifies, but I think that's going a little far. So, yeah, but we did not cover that in the guidelines.

>> Manas Mohapatra: Great. All right, thank you very much.

>> Harley Geiger: Thank you.

>> Manas Mohapatra: So, our next presenter is going to be Jai Haissman. He is the founder and C.E.O. of Affective Interfaces, who are builders of a motion-sensing technology. He founded

Affective Interfaces to build the emotion layer of the Internet and further a new means of human-computer interaction and user interface. Jai's going to tell us a little bit more about how his company utilizes facial detection technology in their product. Unfortunately, we couldn't get his slides loaded. For the archive versions of the Webcast, hopefully the slides will be up there.

>> Jai Haissman: Thank you. Okay, maybe I can act the slides out. [Laughter] And you guys can guess what I'm doing. We do have some very nice demos in the demo booth. I'll

responding, very much personalizing to you. Not feeling so great today? Then it delivers a new iTunes playlist, very different from if you're feeling frustrated or very happy. So, these are t directions that we're moving with our technology. Effectively, it allows us to capture data anywhere and then using just simple off-the-shelf Webcams -- no specialized equipment. And most of the processing can be done locally with our proprietary algorithms. We've done work with Anheuser-Busch InBev and with Proctor & Gamble on market research studies, and we're working with some digital media companies for building this new interactive type of content. So, you might be wondering if you're able to accurately assess emotion, that's very private information. You know, when we have face-to-face contact, then we're able to do that more or less accurately, depending on our own sensitivity and empathy skills. But if we've got devices that are using this, then how can we protect our privacy interests? How can we feel like our own private emotional world is taken care of? So, our policy around that is really about transparency and informed consent and then reciprocity, providing some sort of value -- if we're realizing value -- from the exchange. So, every user knows when the technology is turned on, and they have to authorize turning it on in order for it to be working. And we feel that that's important, from a brand perspective. So, our perspective is really from industry. How is it that we create a context for our technology to be welcomed and perceived as valuable, as opposed to as a privacy threat or as something that's intrusive? People have, more or less, comfort with the technology just based on your own perspective. But creating that basic trust around brand, we think, is very important and also very important for the industry. So, we really encourage those that are involved with these behavioral targeting metrics to shape policy or company policy around that very specifically. Okay, so, let's talk about just why is emotion useful and relevant. Emotion is a fundamental driver to human behavior. So, we're talking about the primers for what we decide and how we associate values to things. We think about our decisions, and how we preference those decisions is largely informed by some kind of emotional tone. "I like this. I don't like this. That makes me nervous. That's really exciting." So, to capture this kind of data involves -- or provides an extremely useful feedback system for enterprise to understand how consumers are responding to their content, to their messaging, through content development. For the user, it provides a very compelling feedback loop for understanding how people -- "How am I doing today, and how's that trending over time?" For government, it's very useful potentially as a truthfulness assessment tool that is likely more accurate than any other existing technologies. There's a lot of work on this by Dr. Paul

Ekman, whose 40 years of research has established that these facial expressions, the microexpressions that we are constantly communicating with, are universal across cultures and are highly reliable indicator of emotional status. So, let's talk a little bit about alternatives to facial expression for understanding emotion. We can use neurofeedback systems that are these dry-sensor headsets, and they track our brain waves and give us a little bit of information about how we're feeling, mostly on the level of excitement and arousal and cognitive processing. But it can't really get down into the emotional brain center because there's too much brain tissue in the way. So, we use behavioral indicators which are hard wired to the emotional brain. The face is displaying how we're feeling in real time. And unless we're trained to mask it, it's a constant broadcast of the internal emotional state. So, that's a very high utility in understanding customer response, but then also for generating self-awareness. So, if you can see a trend line of your happiness or frustration, that's very important. The other applications for the interactive media space we think are extremely promising, this-time gaming content and so on. We're announcing a large data set, which will allow us to do big data calculations on distributed emotion. So, that means if we know how people are feeling based on the area in which they live because they're using our technology, we'll scrub that of identifying information so that it's not personal to that individual. And then we can represent it as regional hot spots for emotion. And we think that'll be extremely useful for predictive health metrics and correlating heart disease to anxiety or depression and then also seeing how markets respond to local changing emotion states. How much time do I have? Okay. All right, so, yeah. I just want to underscore that I think the really important thing we want to bring to this is that we're shaping a culture around transparency and around, you know, informed consent and reciprocity. Thank you very much. [Applause]

>> Manas Mohapatra: I just had a few follow-up questions. You know, you had mentioned the capturing of data and the amassing of this data set. Are the images that you are capturing - are those retained? And if so, then who gets access to those?

>> Jai Haissman: Yes, and it depends on the application. So, in the case of a user where they would like to keep a profile and then have that accessible to them, then we will retain the identifying information. For applications where it's part of a larger data set, then we'll likely scrub it of any kind of identifying information. We've been approached by companies that would like to

have these, I guess, location-based facial tracking of immersive labs or AIM-type applications. And we would not use any kind of identifying information. So, we always have informed consent about our policy and what we're going to do with the data.

>> Manas Mohapatra: All right. I guess the question is, in terms of identifying information, I think there's a question as to whether or not an image of your face is, by its very nature, identifying, and so if that image is actually being retained or shared with anybody.

>> Jai Haissman: Well, the other thing is that we're not doing facial recognition, so there's no identity in the acquisition of the data and the analysis of the data. But we might ask a person for their E-mail contact information. But we're interested in making meaning of facial expressions rather than trying to identify the individual. So, that's fundamentally first.

>> Manas Mohapatra: Great. That's very helpful. Thank you very much. Great. Next we have Andrew Cummins, who's the Chief Strategy Officer of SceneTap. Andrew is a strategy expert in the technology and defense markets and previously worked in multiple strategic development roles at Boeing Defense Space and Security. Andrew and the SceneTap team leverage facial detection technologies and apply them to both data analytics and the social media industries. Thank you.

>> Andrew Cummins: All right. Thank you, Manas. I appreciate it. I hope everyone's doing well this morning. It's a pleasure to be here. I want to thank the FTC for putting on the workshop. As Manas said, I'm Andrew Cummins. I am the Chief Strategy Officer at SceneTap. SceneTap is a data analytics company. We also have a social platform component that's involved. What SceneTap is really doing is we are applying -- we're an example of how you can apply facial detection technology in a unique manner to really produce a positive outcome, commercial outcome, on many different industries. And we are just one example. So, over the next few slides, I just want to talk about a few different areas. First I want to talk about what SceneTap really is,

conversation on really just what SceneTap is in our business so you can have a better understanding of, really, what we do. So, first, SceneTap is really leveraging innovative facial detection technology and we're combining that with our own proprietary systems and we're producing positive benefits in the nightlife industry. So, when I say nightlife, I mean bars, I mean nightclubs,

who individually-- you know, Andrew Cummins. It wouldn't say Andrew Cummins is in "X" venue right now. And then lastly we have relationships with third parties, and really, again, that's just consulting services again using the data and the technology that we have, helping them optimize their business. These are businesses that are, you know, in related and adjacent industries to the nightlife industry. So, you're probably asking yourself now, "How does this technology work?" How do we collect the information? So, really, it's our technology. It's our unique technology system that differentiates us. And so how it works, how we capture the data, is it's -- it's essentially a combination of sensors that are inside the venues, facial detection technology, the AIM Suite technology, people-counting technology. And around this whole thing, we have a proprietary system which is wrapped around the hardware and the software. So, again, what we're doing is we're capturing data in a real-time manner. So, what you'll see on the right-hand side -- On the upper part, you see a graph of what a potential patron, the public, could see on our Website of a venue. So, you can see it says right now -- you know, at that moment, it was 34% full. The average age was 30 of both females and males, and you have a 62% male, 38% female. So, again, aggregated, general basic groups of information. It's just another way to help, you know, make a decision as to what you want to do for that evening. Now, really where the value comes in and where our value proposition is targeted is at the venues. You'll see in the bottom part, this is an example of a graph that we could produce for venues. And again it's this demographic information. We can show trends. We can see what's happening, you know, performance on the last four Thursdays. We can overlay this data with sporting events, weather, if there's events in town, concerts, other types of events. So, whatever it might be. So, they can really get a feel for how their traffic is driven based on the macro environment around them. So, then lastly I really want to end the discussion with the reason why we're all here, with the privacy discussion here. SceneTap really, truly is committed to privacy. As I discussed earlier, SceneTap really does have a proactive approach to ensure individual privacy. We've been operating to the best of our ability within the current frameworks and guidelines that exist. So, just to go over some of our, you know, beyond the AIM Intel Suite that we discussed earlier, to go into some of our own protections that we've built in to ensure individual privacy. First, this is anonymous tracking, okay? We do not track unique individuals, nor do we care about unique individuals at all. This is only grouping people into demographic buckets. Next, it's non-individualized data. We're not sending unique, individualized data points to the public. We're not giving that to the venues. This is all aggregated

data when it's lumped into the buckets, okay? Let's see. So, we do -- All the data is secured. We have a closed-circuit password-protected video feed in each of our venues. So no one within the venue can access any of the data. This is all behind, again, this encrypted, protected system. There are no recorded videos, as Brian was mentioning. There's no recorded video streams. There's no stored images. The data is logged, and then the video itself is actually destroyed on the fly. So, really, the sensors are truly just an eye for the software, and that's all it is. And then lastly, I wanted to talk about transparency because I know that's big issue in this area. SceneTap actually protects -- or, excuse me, you know, works in the area of transparency in two different ways. So, first we do have decals to provide consumer notice. So, in each of our venues, there is actually a SceneTap decal that's in the front window, right by the entrance, okay? So, that essentially gives consumers the opt-out choice that Harley was just mentioning. So, if you can see the SceneTap logo, if you don't want to walk in, that's completely your choice. Secondly, we also have a privacy policy on our Website and on the application. It describes how we collect the data, why we collect the data, what we do with the data. It's available to the public. So, those are the two layers of which we provide this transparency to give consumers the knowledge of everything that we're doing. So lastly, I just want to thank everyone for your attention. I hope you now have a better understanding of SceneTap, how we're using the technology in a unique, creative manner to really leverage this innovative technology to produce positive benefits in different markets and for society. If you have more information, you can please visit us at scenetap.com. If you want to become a user, we'd also appreciate that, as well. And I appreciate your time. [Applause]

>> Manas Mohapatra: Thank you very much. I was just wondering in terms of the decal that you were mentioning, is there anything besides your logo that appears on it -- just the fact that there's a camera or the Website address? Or is it just the logo?

>> Andrew Cummins: It's not just the logo. It provides the Website address, and it also provides pertinent data to the company and kind of what we're doing.

>> Manas Mohapatra: Okay. And in terms of your privacy policy, do you list all the locations that you're operating in?

>> Andrew Cummins: The locations are not, but essentially all of our locations are listed as soon as you enter the front of the Website or the mobile application. They're all listed there, so...

>> Manas Mohapatra: And how many locations are taking advantage of this right now?

>> Andrew Cummins: So, in Chicago, which has been our beta market and our launch market, we've been up and running for about 6 months, and plus 50 venues in Chicago. And actually we are launching the market of Austin, Texas, tomorrow, which we're very excited about that. So, we've got about another 25 to 30 on that market, and hopefully we'll be expanding beyond that.

>> Manas Mohapatra: Great. Thank you very much.

>> Andrew Cummins: Thank you. [Applause]

>> Manas Mohapatra: So, next we have Fred Carter, who, since 2004 has served the Ontario Information and Privacy Commissioner as Senior Policy and Technology Adviser. His primary responsibilities involve providing strategic research, information, and advisory services to IPC commissioners, management, and staff on a wide range of technology and privacy policy issues. Thank you.

>> Fred Carter: Thank you. Thank you, Manas. I'm really grateful for the invitation and the opportunity to talk to you here today. I'm here on behalf of Dr. Ann Cavoukian, who is the information and privacy commissioner of Ontario, Canada. It's our largest province. Dr. Cavoukian has been working in the privacy business for about 25 years, and as a commissioner, this is her third term. She's probably the longest-serving privacy commissioner in the world. Our office is sort of broadly similar to the FTC. We're independent. We carry out investigations. We can issue orders in some cases. We're an ombuds-type organization. We oversee three laws -- access to information, as well -- over the public sector and the healthcare sectors in Ontario. We have a number of functions. What is most pertinent to here is the research and education mandate. Our office is well-known around the world for its proactive views on emerging technologies and their impacts. And in that context, we've been very active. We've done a lot of work in biometrics.

any claim of anonymous, you know, maybe shouldn't be taken at, well, face value, but re identification is always possible, so it's always gonna be important to look at how the technology is

excluded from their gaming facilities because they've got a problem, and they voluntarily enrolled. And the biometric -- sorry, the system in place here, very high-level, is that the challenge is not to identify in any way the hundreds of thousands of patrons that come in out of these facilities, but only to detect them, but only to be able to identify in the most privacy-protective way the people who have voluntarily enrolled, and we're really pleased with the early results. It's very, very encouraging, and this paper describes it. Again, I brought some copies, but they're gone, but it's all available on the Website. So, when you really boil these concerns down, they come down to four what I call meta Fair Information Practice principles -- safeguards, data minimization. That's limiting purposes, limiting collection, limiting retention. We want to see these sorts of things happen. Then, on the other side, user participation -- notice, consent, access, redress. These all speak to the ability of the individual to be a participant in the data life cycle. And then accountability, which is not just to the individual, but to regulators, to other business partners and so on, so forth. We want to see demonstrable adherence to standards as they age, and they seem to be evolving quite nicely. This is the last slide. This is the privacy-by-design principles. You'll see that they comprise seven sort of principles. They map very nicely to the meta Fair Information Practices, with three new additions. Essentially, I encourage you to think of these privacy-by-design principles as sort of a robust implementation of the Fair Information Practices. Set really clear leadership roles. Have verifiable, systematic methods to build privacy into your system, and show the result(ce)5(t)-2(y, w9(,)1(, t)-1(h)1(e4f(c))-1(t)-1(t4)-1((ce)5(t)(u)W(e)- 3(an)1(t)-

>> Beth Givens: Thank you very much, and thank you, Federal Trade commission for convening this event. Just a couple of words about the

say about notice is what I call the euphemism factor, and that is notice that skirts the issue and kind of makes it a happy face, feel-good. Video surveillance you may have seen these for your

>> Manas Mohapatra: Thank you very much, Beth. I'm sorry. We had a lot to get through today, and I was hoping for more opportunity for facilitated discussion. And in light of the lack of time, I was just wondering if people on the panel had, you know, closing thoughts, if there are things that they'd like to respond to that have been spoken. If we just want to start with Brian, if you do, if you want to chime in or move forward. Harley?

>> Harley Geiger: So, Beth, I wanted to respond to a couple of the things that you mentioned in your presentation. You had said that the digital signage privacy guidelines, which I actually had written, lack specificity. But I actually think that they're very extremely detailed. I have them with me, and I invite anyone to read them. But it covers specific categories of synonymous data and direct identifiers that are not covered in other codes, including the POPAI code. It gives specific notice language. I also would like to hear more on how your troubles about having an opt-out notice for facial detection. So, that was a very difficult thing to sort of implement, but we had three layers of notice, and it's difficult to think of another way to notify consumers and have them avoid facial detection without simply outright banning facial detection in a given area where it might be otherwise appropriate. I mean, obviously, a locker room, HIPAA-covered entity, might not want to have facial detection, but a place like a mall, without banning it, how, if you don't have a privacy policy, a notice at the perimeter and a notice at the device, are you to implement and opt out? And, lastly, still on notice -- in fact, the digital signage privacy guidelines are quite protective when it comes to notice. The POPAI guidelines, unless they've been changed, I believe they just have one notice covering an entire establishment, whereas for our guidelines, we have one, and each device, it's actually doing the collection.

>> Beth Givens: Yes. Facial detection, I guess it boils down to the creepiness factor. Facial detection I actually think would be offensive to a considerable number of people, and I think the notice Is actually incredibly important. I was going to suggest, and I will now, that in addition to the text notice -- By the way, again, other languages, ADA-

>> Harley Geiger: It is ADA-compliant. The guidelines are ADA-compliant.

>> Beth Givens: Yeah, yeah. But I was thinking it might be useful to have a QR code, as well, so the --I think, what, those can accommodate, what, 4,200 or so characters? That would be like an eight-page privacy policy. For those with smartphones, could learn even more. And I think with digital signage, it's enough of a new thing for many individuals that they might benefit from learning more and just capturing it on their smartphones with a QR code.

>> Harley Geiger: So that would ease your concern about the opt-out notice, to have a QR code on the notice?

>> Beth Givens: Actually, it doesn't ease my concern about, you know, just don't go into those establishments if you are uncomfortable with facial detection or facial recognition. That I do think is kind of a cop-out. And one of the things I wanted to say -- and, again, I'll say it now -- brilliant minds have gone into the development of these technologies, both on the science and technology side and on the business side. I would love to see those brilliant minds working towards a creative and effective notice mechanism for digital signage. I think that would be very, very constructive.

>> Manas Mohapatra: Just one follow-up question, just related to the facial detection. I'm just wondering what the panelists thought about in terms of should there be some prohibited uses of facial detection -- for example, differential pricing based on somebody's age or their gender or, you know, to the extent that ethnicity is possible? Is that something that, you know, should come out? Is that something that should be prohibited? Is that something that industry should just be aware of? I'm just wondering if people have thoughts on that?

>> Harley Geiger: Well, yeah. We would have major concerns about it, and, you know, we would have to gather more information and talk to the company. But on its face, that sounds like something that we would want prohibited, sure.

>> Brian Huseman: I mean, and that's an issue that's -- I mean, not just in facial detection, with Internet purchasing, I mean, with a bunch of different technologies.

>> Jai Haissman: And that's, again, why CDT recommends not just having facial recognition specific legislation. All of the ways that Fred just mentioned that you can be tracked and identified will still be viable if you just have facial recognition specific legislation, so it needs to be wrapped into consumer baseline privacy legislation that covers all of those categories for it to be effective at all.

>> Brian Huseman