CALIFORNIA PRIVACY PROTECTION AGENCY BOARD

PRE-RULEMAKING STAKEHOLDER SESSION - LOS ANGELES

AUDIO TRANSCRIPTION OF RECORDED PUBLIC MEETING

MONDAY, MAY 13, 2024

LENGTH: 1:48:25

Transcribed by:

iDepo Reporters
898 North Pacific Coast Highway
Suite 475
El Segundo, California 90245
(808) 664-6677
www.ideporeporters.com

APPEARANCES:

Present: ASHKAN SOLTANI, Executive Director

PHILIP LAIRD, Meeting Counsel

NEELOFER SHAIKH, Attorney for CPPA

KRISTEN ANDERSON, Attorney for CPPA

MEGAN WHITE, Deputy Director for Public and External Affairs

LISA KIM, Senior Privacy Council and advisor

ZACH PEREZ, Professional Artist

NOEMI LUJAN PEREZ, President and CEO of ECODiversity

LINDSEY TONSAGER, Covington & Burling

ALBERT LOWE, UFCW Local 770

ANDREW DRULY YOUNG, Artist

TASIA KEEFER, LA County Business Federation

ELIZABETH GUILLOT, CrowdStrike

TOM ROSS, Board member of the United Chambers of Commerce, Government Affairs Committee, and San Fernando City Chamber of Commerce member

KRISTEN WALKER, Professor of Marketing and MBA Director at Cal State University, Northridge

MANUEL PLANK, Illustrator

SOP KAMAL

KIM OWENS, Entrepreneur

MR. SOLTANI: Hey everyone. Thank you for coming. My name is Ashkan Soltani. I'm the Executive Director of the California Privacy Protection Agency. Excited to have you all attend our first stakeholder session on this session. As you all know, Automated Decision-making and Privacy are important issues that touch nearly like every aspect of Californian's lives. We're eager to hear from you all about your thoughts on our regulations.

Just for background, for those not familiar with our Agency, California Privacy Protection Agency was established in 2020 when the voters voted to approve Prop 24. Our Agency is tasked with free missions, rulemaking, raising awareness and enforcement of the California privacy -- California consumer privacy, and the first comprehensive consumer privacy law in the US.

Already, our Agency has taken following steps to fulfill our mission, including passing, implementing regulations in March, 2023, but further clarify consumers' rights with respect to the CCPA and business' obligations under that law. We're also working on developing regulations that govern Automated Decision-making Technology, including those leveraging artificial intelligence as well as Risk Assessments and Cybersecurity Audits. As you may be aware, the Agency has been working on this topic because quite some time. Starting in fall 2021

we brought our initial pre-rulemaking on this topic.

Today is yet another important step in the stakeholder engagement that leads to the final regulations. This is an opportunity to learn and provide preliminary feedback on the Agency's proposed regulations. So just an overview, just so -- and a reminder, these are draft regulations, and I don't speak for the Agency or the Board, not at the Board taken formal position on these regulations. We today wanted to simply help outline our approach and importantly hear from you. The next steps pursuant to the CPA Board's -- CPPA Board's direction, we may move into the formal rulemaking step, but that's the next step being a longer process.

During that -- during that process, you'll have another opportunity to provide formal comment. Once draft regulations enter the formal rulemaking process. And again, you don't want to take away from the legal team's presentation. They'll go over at length at this point on. But everyone now, this is just an opportunity to hear from us and from us to hear from you. I'm joined here my wonderful staff today. Here with me are our general counsel, Phil Laird, Neelofer Shaikh, our attorney, Kristen Anderson, attorney, Lisa Kim our senior privacy council and advisor and Megan White in public affairs.

Just to give you a brief overview of today's

agenda, our legal team will provide 45 minute presentation around our approach to Automated Decision-making, Cybersecurity and Risk Assessments. Then we'll open up some comments from you all. Megan will provide a bit more detail on our presentation, but each member of the public will have five minutes to speak. If you think there's more that you want to share or something else we should hear about. We also are having two other stakeholder sessions, one in Fresno next Wednesday, and then one again in Sacramento next week and that being will be hybrid. So you can join in person or via Zoom.

In some instances, we may respond to a question at the end of the event, but our primary purpose today is to listen and hear your feedback. Now, please note we can't get legal advice and these portfolio regulations are draft, so there's some limitation to what we can share. So a couple other notes. This video is not being live streamed, but it is being recorded and the recordings will be posted to the CPPA website after the meeting, so others can hear questions and answers. Now with that, I'll hand it over to Megan, talk about a little bit of housekeeping.

MS. WHITE: Hi everybody. My name is Megan White. I'm the Deputy Director of Public and External Affairs. Thank you so much, Ashkan. Just a couple of housekeeping notes for everybody. As you can tell, we don't have mics

here, so if you have trouble hearing, obviously there's seats up here. Feel free to come up closer or you can always raise your hand. Our team members will definitely try and project a little bit more. Emergency exit for any reason we'll head out those doors and back out the front just as you probably came through, so right by the metal detectors.

If you need a restroom right through these doors. And then you're going to make a right. There's the men's and the ladies room as well. If you didn't have a chance, you can grab our handouts. We have them in English and Spanish on the front table. And if you'd like to sign up for any of our e-mail links, you can certainly add your e-mail there. We're happy to add you.

Regarding public comment, we would love it if you felt comfortable to come up to the podium. It's going to help us capture what you said (inaudible) because we want to make sure that we're capturing everybody's feedback. It's optional, but we prefer if you did that because the mic will be able to pick you up a little bit better. You're going to have five minutes for public comment, so as soon as you begin, I'll start the timer. I'll do my best to get your attention and tell you when you have one minute left and then you'll hear it ding when you're at five and we'll have to wrap you up.

And if we have any non-English speakers here, Spanish is your preferred language. We have our wonderful translator, Diego in the back. He's happy to translate for you. So if you feel comfortable, please let us know if you'd like translation services and we have that here for you. Outside of that, any general questions anybody has at this point, just housekeeping stuff. Okay, lovely. Then I'm going to pass it over to our team to get you going.

MR. LAIRD: Good afternoon, everybody. As mentioned earlier, I'm Phil Laird, the general counsel here at the Privacy Protection Agency. And welcome to the first of our first three pre-rule making stakeholder sessions that we're doing statewide. Now we're hosting these for two main reasons. The first is we really want to provide more information about these draft regulations to a broader population. We want to reach more consumers, more businesses, and more practitioners about what we're doing right now and the top on the topics of Automated Decision-making Technology, Risk Assessments, and Cybersecurity Audits.

But second, we also really do want to hear from you about our draft regulations before we move into formal rulemaking, we'll be explaining kind of what that means and where we are in this process. But this is to say feedback now is welcome. Feedback later is welcome. All the

feedback we can get is great. We really are happy to have you here and we're looking forward to hearing that feedback once we've gone through our presentation on what these regulations do.

And then, because I'm the lawyer, I also have the lawyer's disclaimer. So before we get started in earnest, I do want to be clear, and you've already heard our director say this that the CCPA requires us to issue these regulations on Automated Decision-making Technology, Risk Assessments, and Cybersecurity Audits. I'm going to go ahead and do us a favor right now and tell you instead of saying Automated Decision-making Technology time and time again, I'm just going to refer to it as ADMT going forward. So will my colleagues as well. But that's what we're referring to when we use that acronym.

Now when we talk about these regulations, where we are at this point is we have drafted these regulations as an Agency, but we have not yet started formal rulemaking. And the formal rulemaking process in California does have many steps and there are additional opportunities for public comment during that period which we'll talk about more at the end.

But our presentation today is to explain the draft regulations so you can understand them and to help you participate in the rulemaking process once it kicks off. So

again, to be clear, these regulations are not in effect today. These regulations haven't even been approved by our Board to go into effect at a future date. They are draft regulations that the Board is currently considering and that there will be further discussion and activity by the Agency and by the Board on these regulations going forward.

And finally, as mentioned before, even though it's three lawyers up here, we are not actually providing legal advice to any of you. Businesses seeking to ensure compliance with the law should consult the statute regulations that are currently in effect and their own legal counsel. And finally, I'll note that the opinions we express today are our own and not necessarily those of the Agency, it's Board or any individual Board members. The way it works is our Agency is overseen by five Board members and only those five Board members can collectively make decisions for our Agency including on whether or not to adopt these draft regulations.

Okay. So you've already heard our agenda a few times. You've maybe seen it. I'm going to run through it very quickly one last time. So as you can see from the slide, we're going to cover several topics today. First, we are going to provide a little background on our Agency, who we are and why we're talking about these things. And then we're going to walk you through these draft regulations I've

been referring to on ADMT, Risk Assessments and Cybersecurity Audits. And then we will conclude with information about how you can participate in that formal rulemaking process that I was referring to earlier.

But after we're done, we still want an opportunity now, since you're all here to hear from you now on these draft regulations. And as was mentioned, we will limit comments to five minutes person. But really we're excited to hear from you. This is meant to be a listening session and we'll be -- we'll be eagerly kind of taking notes and kind of listening to all the feedback we get today.

Okay. So to give you a quick background on the -- our Agency as well as the law we enforce and our current activity, I'm just going to give you now a brief history of who we are and why we're here today. So as you can see, we have this great little timeline of events. The California Consumer Privacy Act, the CCPA, it's a lot of acronyms, I apologize for that. But it passed in 2018. It went into effect in 2020. And it was the first comprehensive consumer privacy law in the nation. It gave consumers rights over the personal information that businesses collect about them, and it required businesses to inform consumers about how they collect, use, disclose, and retain personal information.

Now, jump forward to November, 2020 and you might

have remembered that there was Proposition 24 on the ballot and California voters approved Proposition 24, which enacted something called the California Privacy Rights Act, the CPRA, which amended the CCPA. This is all to say lots of acronyms for the law though that we enforce, which is the CCPA, the California Consumer Privacy Act.

And so those amendments then took effect in 2023. And now the CCPA additionally provides privacy protections to employees, independent contractors and job applicants, which is sort of a rare feature in privacy laws across the country. And it also now includes new rights for consumers, the right to correct inaccurate personal information that a business might have about you, the right to limit a business' use and disclosure of your sensitive personal information. And as we'll be discussing today, the right to access information about and opt out of a business' use of Automated Decision-making Technology or ADMT including profiling. We'll define that later and explain what that means.

The amendment's also created in our Agency, the California Privacy Protection Agency. The Agency is tasked with implementing and enforcing the CCPA, the law I was referencing earlier, and that includes regulations that implement the CCPA's requirements. So we're here today because we're going to talk about some of those draft

regulations that we are considering here at the Agency.

So as an Agency, we have actually a lot of sort of components to our mission, but it boils down really to three key roles and that is rulemaking the kind of regulations work we're talking about to today, promoting public awareness about these very important privacy rights that all Californians have, and an auditing and enforcement function to ensure that businesses are complying with these laws and regulations and it gives us the ability to investigate and enforce any violations that are discovered.

So moving on into what we're doing today we're kind of doing the first two things I mentioned. We're talking about regulations and we are also trying to promote public awareness. As we've been saying today, these regulations are not in effect and we haven't started the formal rulemaking process. We are what we would consider the preliminary rulemaking stage. During preliminary rulemaking, we invite public input.

At this stage, we're seeking feedback on these draft regulations and once we're through this presentation, we'll invite you to share your thoughts. Later during formal rulemaking, there'll be another opportunity to make additional public comment and I'll explain that in a little bit. And so with that said, I'm going to stop talking and I'm going to turn it over to my real better halves over

here. Beginning with I believe Kristen, you're -- Neelofer, you're kicking it off. All right.

MS. SHAIKH: Thank you. So as our general counsel mentioned the CCPA directs our Agency to issue regulations governing access as opt-out right, related to business' use of Automated Decision-making Technology. So today we're going to spend some time talking about what ADMT actually is, so what it includes and what it does not include. We'll also talk about when a business would need to comply with the proposed requirements for Automated Decision-making Technology. Importantly, these requirements would not apply to just any use of ADMT, it would only apply to certain uses that we'll be talking more about. Lastly, we'll talk about what those specific requirements for those uses of ADMT would be.

All right. So turning now to what is Automated Decision-making Technology that is mouthful. And so we're just going to break it down into four components. So the first thing is that it has to actually be a technology that processes personal information. So it needs to collect, use, retain, disclose, or otherwise handle personal information in some way. It also needs to use computation and most importantly, needs to use that computation to replace or substantially facilitate human decision making.

So we use that term substantially facilitate.

That means that the output of that technology is a key factor in a human's decision making. So for example, if the business is using technology to generate scores about consumers that a human reviewer then uses as a primary factor to make a decision about that consumer, that would be a type of ADMT because that technology is substantially facilitating human decision making.

Lastly, ADMT includes profiling, which we're -- we'll talk more about on the next slide. Examples of Automated Decision-making Technology includes things like resume screening tools that businesses use to decide which applicants they want to hire, facial recognition technologies that businesses use to verify the identity of consumers as they enter, for instance, a workplace, and tools that place consumers into audience groups to target advertisements to them.

Lastly, please note that ADMT does not include routinely used technologies. So things like calculators, spell checks, spreadsheets, these things are generally excluded from the definition of ADMT. And if you want that full list of the technologies that are excluded, you can look at our proposed regulatory text, which is available on the CPPA's website.

All right. Now what is profiling? As I mentioned previously, ADMT includes profiling, that generally is

broken down into two elements. So first you need to be engaging in automated processing of personal information and that automated processing has to be done to evaluate someone. So that includes, for instance, analyzing or predicting a consumer's ability to do or be something, their reliability, their health, their economic situation, their interest, their behavior, their location. That is what is an -- you need to be doing automated processing to evaluate a person in those ways to be engaging in profiling. And that would be a use of Automated Decision-making Technology.

Now, as I mentioned before, even if a technology is Automated Decision-making Technology, that does not mean that it would be subject to the proposed requirements. Generally, you first need to be a business under the CCPA. That businesses generally are for-profit entities that meet certain requirements under the CCPA. So for example, making over a certain amount of money in annual gross revenue could lead to you being a business. And for those of you who are unsure, if you are a business under the CCPA, we have helpful fact sheets available on our website. And of course you're always welcome to look to the existing law, including our regulations.

Now, assuming you are a business under the CCPA, you also need to be using ADMT in one of three ways, which we're going to talk more about. That would be using ADMT

for a significant decision to engage in extensive profiling or for training uses of Automated Decision-making Technology. Turning to the first use case, a business using ADMT for a significant decision concerning a consumer.

So what is a significant decision? These are decisions that have important consequences for consumers. So for instance, the decision to terminate them or suspend them from their job would be a significant decision. We provided a list of examples on this slide of what different types of significant decisions are, and you're again, welcome to look at the full list on both our fact sheet and in our proposed regulation.

As an example, if a business is using a video screening technology as part of its job interview process and that technology is analyzing job applicant's body language, their facial expressions or their gestures to determine whether they would be a good employee and should be hired, this would be a use of ADMT to make a significant decision, in this case, hiring about a consumer. Next slide.

The second use case we're going to talk about is the use of ADMT for extensive profiling. As I mentioned before, profiling generally refers to that automated processing personal information to evaluate someone such as their personality, their interests, their behavior. We're

going to talk about three types of profiling as extensive profiling. The first is work or educational profiling. This is profiling someone who's acting as a job applicant, a student, an employee, or an independent contractor through systematic observation. So for instance, using a productivity monitoring software to track how quickly workers are completing projects would be an example of work profiling.

The second is public profiling. So this is profiling consumers through systematic observation of a publicly accessible place. So for example, deploying a facial recognition technology in a stadium or in a mall. Lastly, profiling for behavioral advertising. This is profiling a consumer to target advertisements to them. So those three would be extensive profiling.

Training for the last use case, which are the training uses of ADMT. A business would be subject to the ADMT requirements, which we'll talk about next for training uses of ADMT, which generally means that a business is using consumer's personal information to train an ADMT for certain purposes, specifically to make significant decisions. So for instance, that would be training ADMT that's used to make decisions about which consumers would be offered business loans. To identify people, so that could be training of facial recognition technology. For physical or

biological identification or profiling, we're going to talk a little bit more about that term.

But this would include for instance, training a technology that analyzes people's facial expressions or gestures to infer their emotional state. And lastly, to generate deepfakes, which some of you may have heard about in the news, this would be training ADMT that could generate, for instance, fake images of real people that are presented as truthful or authentic.

Now my colleague, Ms. Anderson, is going to talk about what the actual proposed requirements would be for these three uses of ADMT by businesses.

MS. ANDERSON: So only if a business is using ADMT for significant decision, extensive profiling or training uses, would it have to comply with (inaudible) requirements for ADMT. Specifically, the business would have to provide a pre-use notice to the consumers whose personal information it wants to process using the ADMT. It would have to give consumers an easy way to opt-out of its use of the ADMT, and it would have to give consumers an easy way to access information about how the ADMT was used with respect to them, which the consumer can exercise later if they proceed with the business's use of ADMT. We'll now talk about each of these requirements in a little bit of more detail.

So the first is before business can use ADMT in

any of those ways that we just discussed, it must provide a pre-use notice to the consumer so that the consumer can decide whether to opt-out or to proceed and whether to access more information about the business' use of the ADMT. The pre-use notice would have to include why the business wants to use the ADMT and it would have to be the specific purpose, not something like to improve our services. It would also have to provide information about how the ADMT would work. That includes information such as the logic used in the ADMT, including the key parameters that affect its output. It would have to include the intended output of the ADMT.

So for example, if the ADMT creates a score or does it place them into a specific profile or segment, that would be the output. It would also have to include how the business plans to use that output, including a role of human involvement. For example, if a business plans to use the output score that a resume screening tool generates to determine who will be offered an interview, the business would need to disclose that that's how it's planning to use the tool and the role of any human reviewers in that process.

The previous notice would also have to include a description of a consumer's right to opt-out and how they could exercise that right. It would also include a

description of the consumer's right to assess, more information about how the business used the ADMT with respect to the consumer if consumer proceeded with the use of ADMT at that time.

Finally, the pre-use notice would have to include that the business is prohibited from retaliating against consumers for exercising their CCPA rights. If a consumer opts out at the pre-use notice stage, so before the business uses the ADMT, the business is not allowed to start processing the personal information, using that ADMT. If the consumer went ahead with the business' use and decides to opt out later, then the business has to immediately stop processing their personal information using the ADMT and inform anyone else that may have involved in that ADMT such as service providers or vendors that they need to stop as well.

There are exceptions to when a business must provide an optout, which we'll talk about next. One thing to note here though is that there's no exception to profiling for behavioral advertising or for those training uses of ADMT. A business would always have to provide an opt-out from its use of those types of ADMT. Next slide.

The first exception is a security fraud prevention and safety exception. It applies when a business wants to use the ADMT for profiling in the workplace or in

educational settings or in public.

In these cases, a business would not be required to provide the ability to opt-out of its use of ADMT if it was using it only for security, fraud prevention and safety. To rely upon this exception, the business cannot be using the ADMT for any other purpose besides security, fraud prevention and safety. The second exception is a human appeal exception. It would apply when a business wants to use the ADMT can make a significant decision concerning a consumer. The business would not be required to provide the opt-out if it provided the consumer with the ability to appeal the decision to a human decision maker.

To qualify for this exception, the business would have to generally provide the consumer with a method to appeal to a qualified human reviewer who has the authority to overturn the decision. The business also would have to clearly describe to the consumer how they could submit their appeal and enable them to provide information for the reviewer to consider.

The third category of exception is the evaluation exception. This would apply when a business uses ADMT for admission, acceptance or hiring decision for allocation or assignment of work and compensation decisions or work or educational profiling. The business would not be required to provide the opt-out if the business has evaluated the

ADMT to make sure that it works as intended for the business' proposed use and does not discriminate on the basis of protective classes. It would also have to implemented accuracy and non-discrimination safeguards.

Okay. So if a consumer proceeds with the business' use of ADMT, they can then request access to more information about how the business will use the ADMT with respect to them. So if a consumer requests that access, the business' response to them would have to include the following. First, why the business used the ADMT. And again, this would be the specific purpose.

Second, how the ADMT worked for that consumer. This would mean providing the consumer with the output of the ADMT with respect to them. So if the technology generated the score, for example, the business would provide the consumer with their score. It would also include how the business used the output with respect to that consumer. So if it were to make a significant decision towards running the consumer for example, that would include the role of the output. So the score plus the human involvement in the use of that score. It would also include the logic of the ADMT, again, including the key parameters that affected the output and how those applied to the consumer.

Third, it would include the business' prohibited from retaliating against consumers for exercising their CCPA

rights and instructions to the consumer on how they can exercise those rights, like the right to correct. I'll note here that the business that's using personal information to train ADMT would not be required to provide an access response to the consumer. In addition, a business that makes an adverse significant decision using ADMT will have additional notice requirements. An adverse significant decision would include something like being demoted or terminated from a job, denying someone housing or essential goods or services.

And the additional notice in these instances is necessary to ensure that consumers know when a business has made a significant adverse decision about them using ADMT. There may be a long time between when they get the pre-use notice and decide to go forward and when the business actually makes that significant adverse decision. In addition, consumers might not want to exercise their right -- their access right unless the business uses the ADMT to make a significant adverse decision about them. So these additional notices make the consumer -- make the consumer informed so that they can decide whether to exercise their access right or not. Next slide. Great.

Lastly, if a business is using physical or biological profiling for significant decisions or extensive profiling, they would have additional requirements. So what

are we talking about when we say -- when we use this term? It generally refers to evaluating people using ADMT with information about their physical or biological characteristics. Examples of this include facial recognition technology because that's analyzing your face to identify you. It would also include things like a motion assessment tool that evaluate your eye movements or other facial movement for gestures to analyze or infer your emotions or behavior.

So a business of using this kind of physical or biological identification or profiling for a significant decision or for extensive profiling must first evaluate that technology to make sure that it works as intended for the business' proposed use and does not discriminate on the basis of protected classes. And the business must implement accuracy and non-discrimination safeguards.

MS. SHAIKH: So we're now going to turn to risk assessments. Before we move on to the next section. For folks in the back rows, if you cannot hear us, just raise your hand. We'll make sure -- thank you -- thank you for that thumbs up. I appreciate it. And then for folks in the front rows, if you feel like we're screaming at you, just let us know as well and we'll tone it down. So now turning to risk assessment.

A risk assessment for those who have never done

one before or just haven't heard of this term, it generally involves identifying risks in this case to consumers' privacy for a given activity and mitigating those risks. And the goal of a risk assessment is to make sure that businesses don't do things with consumers' personal information when the risk to consumers' privacy outweighs the benefits of that activity.

So, turning now to who actually would need to conduct a risk assessment similar to a proposed ADMT requirements, you'd have to first be a business under the CCPA and assuming you are a business, you would need to conduct a risk assessment before doing any of the four things on this slide. So, first selling or sharing personal information, second, processing sensitive personal information.

And when we use that term sensitive personal information, we mean things like your social security number, certain financial information that you have, your precise geolocation, your health information. And it will also include children's personal information. So that is the personal information of consumers that a business knows to be under 16 years old.

In addition, if you're using ADMT for significant decision. So remember, those are those decisions that have important consequences for consumers that we talked about

earlier, such as hiring them or firing them, or extensive profiling. So that's the worker educational profiling, public profiling, profiling for behavioral advertising. If you're using ADMT in those ways, you would also need to conduct a risk assessment.

And lastly, if you are training Automated Decision-making Technology or artificial intelligence in certain ways, you would need to conduct a risk assessment as well. These ways are on your fact sheets, but I'll just say them quickly again now, this would be training ADMT or AI for a significant decision to establish individual identity. Things like facial recognition technology for physical or biological identification or profiling, training AI or ADMT that's capable of generating deepfakes about people as well as training ADMT or AI that can operate generative models.

So now that we've talked about when -- what activities would trigger a risk assessment, we're now going to talk about what actually needs to be in those risk assessments. At a high level, a risk assessment would need to include first why the business actually needs to do that activity. So what's the purpose of it.

Second, it would need to include the types of personal information that the business would need to collect, use, disclose, retain or otherwise process to do the activity, including whether it involves sensitive

personal information.

Third, it would have to explain how the business would actually do the activity. So these are the important operational elements of that activity. Things like how many consumers, personal information the business would need to collect, what disclosures the business has actually made to those consumers about the use of their personal information. Who else might be involved in the activity, what types of technology the business plans to use to do the activity. These operational elements are all important to identify because they can affect the risk to consumer's privacy. And so identifying them is a critical part of conducting the risk assessment.

In addition, for uses of Automated Decision-making Technology for significant decisions or extensive profiling, the risk assessment would also identify additional information about how the technology works. So this would be the logic of that technology, what that output is, and how the business plans to use that output to make those decisions.

Number five is really the crux of the risk assessment. This is the heart of it where the business would identify what are the benefits of that activity, and importantly, what are the consequences to consumers? So what are the negative impacts to their privacy that could

result because of that activity? And accordingly, what are relevant protections that the business wants to put in place or already has put in place.

Lastly, the business would identify whether it would initiate the activity. So what's the confusion here? Is the business going to go forward? And what are the details about who contributed to reviewed and approved that risk assessment and when? An important note here is, as I mentioned before, the goal of a risk assessment is to ensure that businesses are not engaging in activities where the risk to consumers privacy outweigh the benefit. And so a business would be prohibited from starting any of those four activities I talked about if the risk to consumer's privacy outweighed the benefits of that activity.

But turning now to the timing requirements. So when would your business actually conduct or update the risk assessment? So first, you would conduct a risk assessment before you started any of those four activities. And that makes sense because it's -- the goal again, is to identify risks and place mitigation. You want to do that before you start not midstream. And then a business would also need to review those risk assessment at least once every three years to making sure that they remain correct and update them as needed.

And then lastly, if something important has

changed about how you conduct the activity. So for instance, if your business has identified that it needs to collect more sensitive personal information about a consumer, the business would need to immediately update its risk assessment to identify any additional risks to consumers' privacy and implement appropriate safeguards.

Now that we've covered what a risk assessment would include and when a business would conduct or update one, let's talk about what a business would actually have to submit to the agency. So one of the requirements on th e CCPA is that a business would have to submit its risk assessment to the agency on a regular basis. So we're going to talk about what would need to be submitted and when.

So a business would need to submit a certification of compliance. This is a certification by the highest ranking executive at your business in charge of risk assessment compliance. The business before starting any of those four activities we talked about has conducted a risk assessment.

In addition, the business would submit abridged risk assessments. So as with the term, abridged these risk assessments in short form. So for each of your risk assessments, the business would submit an abridged form of it that would identify the relevant activity. So for instance, of those four activities, are you selling or

sharing personal information processing sensitive personal information using ADMT in the ways we talked about or training ADMT or AI for those purposes, we've discussed.

If so, you would identify that activity, you would identify the purpose of the processing, you would also identify the categories of personal information that were actually used for the activity. And lastly, the relevant safeguards are protections that your business has put in place for that activity. Those will be in the abridged risk assessment for each risk assessment conducted, and those would be submitted to the agency.

When would these materials be submitted? So a business would have 24 months from the effective date of these regulation to submit that first certification and the first batch of abridged risk assessments to the agency. After that, the business would submit them annually. So every calendar year after that first submission, the business would submit its updated or new risk -- abridged risk assessments and its new certification.

Lastly, for the unabridged risk assessment. So if this is the full risk assessment, a business would have 10 business days to submit them to the agency or the California Attorney General if the agency or AG requested it. Great.

Lastly, one important thing that we just want to note here. We are aware that other states and other

countries have their own risk assessment requirements. You might hear these called data protection assessments or data privacy impact assessments. If you are a business that is already doing risk assessments to comply with those other laws, we want to make sure that you know that you do not have to redo it or duplicate it for the CCPA, you could use the same risk assessment for the same activity to comply with other laws and the CCPA. However, we want to note that if that risk assessment did not meet all of the requirements of the CCPA regulations, the business would need to add to it as dated.

All right. I'm now going to turn it off to turn it -- turn it to Ms. Anderson for some illustrated examples of how these things all work together.

MS. ANDERSON: It's okay. So now we hop through two examples of business activities and what the business would have to do under these risk assessment and ADMT requirements that we just walked through. These examples don't cover all potentially applicable laws or enforcement circumstances. Still without the examples could be useful for businesses seeking to understand how the draft regs would apply under certain circumstances. So our first example.

MS. SHAIKH: (Inaudible).

MS. ANDERSON: (Inaudible). Okay. So our first

example is a retailer that wants to use facial recognition technology in its stores to identify shop ledgers. So what would the retailer be required to do under the proposed regs? It would have to conduct a risk assessment, evaluate the facial recognition technology to ensure that it works as intended for the retailer's use, and does not discriminate on the basis of protected classes. It would have to implement accuracy and non-discrimination protections. It would've to provide the pre-use notice to consumers. It would've to provide consumers with the ability to access more information about the use of ADMT, but the retailer would not have to offer an opt-out from its use of ADMT as long as it uses that facial recognition technology only for fraud prevention in this case.

All right. Our next example. Our second example is a business whose HRP wants to use a spreadsheet to input junior employees' performance evaluation scores from their managers and colleagues, and then calculate each employee's final score that the manager will then use to determine which of them going to be promoted. So what would the business be required to do under our proposed regulations? It would not have to conduct a risk assessment, and it would not be subject to the ADMT requirements because if the business would be using the spreadsheet merely to organize human decision makers evaluations, this wouldn't be ADMT

under our definition. Recall, the ADMT requires the business to use technology to replace or substantially facilitate human decision making.

Now that we've ticked through those we'll move on to cybersecurity audits. Our proposed cybersecurity audit regulations are designed to ensure that vision decision meeting certain thresholds independently and thoroughly assess how they protect consumer's personal information on an annual basis. Taken together the proposed requirements will help businesses to identify and mediate problems in their cybersecurity program resulting in further protections for consumers.

So today we're going to cover who would need to conduct a cybersecurity audit, what a business and the business' auditor would have to do to complete an audit. And that would include things like how the business would complete the audit, who would the auditor be and what they would have to do, what the audit itself would include, and when the business would have to complete the audit, likely.

So starting with who would need to complete a cybersecurity audit, assuming you're a business, as we've talked through before, if you're a business under the CCPA, you'd also then have to meet one or both of these two thresholds to be subject to the cybersecurity audit requirements, meaning that you would need to complete an

annual cybersecurity audit.

The first threshold is a business that made more than half of its annual revenue in the prior year from selling or sharing consumers personal information. The second is a business that made over $28 million in annual gross revenue in the preceding year and processed personal information of 250,000 or more consumers or households in the preceding calendar year, or processed the sensitive personal information of 50,000 or more consumers in the preceding calendar year.

And as Neelofer touched upon earlier, SPI is being expanded to include the personal information of consumers that the business had actual knowledge were under 16 years of age. So if you're subject based requirements, how would you actually complete a cybersecurity audit? There are four main things that a business would have to do to complete the audit. First, it would have to select its auditor. Note that the auditor does have to meet certain requirements, and we'll cover those in the next slide.

Second, the business would have to provide all information the auditor requests as relevant and not hide important facts from them. This is to make it possible for the auditor to complete a thorough audit using their own judgment and the information that they consider necessary.

Third, the business would have to report the audit

results to the senior most individuals in the business responsible for cybersecurity. There would be guardrails to make sure that the business didn't improperly influence the auditor as they complete the audit. But at the end of the day, the people who are responsible for cybersecurity audits -- sorry for cybersecurity overall, need to know the audit results so that they can understand how they're doing and where to focus their attention to better protect consumer's personal information.

Finally, the business would have to submit a certification of completion to the agency through the agency's website. That certification would be signed by the most senior individual in the business for responsible for cybersecurity audit compliance. He would certify that the business has completed the audit as set forth in the draft regulations and that they've reviewed and understand the audit's finding.

Okay. So who could the auditor be? As we just discussed, the business has to select the auditor, but the auditor cannot just be anyone. The auditor has to be qualified, unbiased, and independent, and they have to be a professional using professional auditing standards and procedures. Those are generally accepted in the -- in the profession of auditing. The auditor could be someone working in the business or it could be an external auditor.

So if the business already employs somebody who meets these requirements, that person could be the cybersecurity auditor.

Now, what would the auditor have to do? Since we've covered who the auditor can be? The three main things that the auditor would have to do to complete the audit are as follows. First, they would have to determine which of the business' systems would need to be audited and how to assess them. They would do that, likely based upon their expertise and the information provided by the business. That information would include things like where and how the business collects, processes, stores, consumers' personal information.

Second, the auditor would independently review documents, conduct tests, and interview people to support and assess their cybersecurity program. The draft regulations list the parts of a business' cybersecurity program that the auditor would have to assess, document, and summarize, and we'll cover some of those as well as what the audit would need to include on the next slide.

Third, the auditor would have to certify that they completed an independent and an unbiased audit. Okay. So we've just talked about what the auditor would have to do at a high level. And the next two slides talk more about what the auditor would have to include in their audit report. We

break down what an audit would have to include into eight key pieces. First, the audit has to include a description of the systems audited.

Second, the audit would have to include the information the auditor used to make their decisions and why it supported their findings. That would include things like why they scoped the audit the way they did. So why if some for in scope and others out of scope, why they assessed the systems and components the way that they did, the evidence that they examined to make their decisions and assessments, for example, which documents they reviewed, the kinds of sampling and testing they performed, and the interviews they conducted, and why all of this was appropriate and sufficient to justify what they found.

Third, the audit would have to include the auditor's assessment of how the business protects consumers' personal information. That includes the written documentation of the business's cybersecurity program. So things like the written policies and procedures that also includes the common ways that businesses protect consumers' personal information like how it authenticates employees and customers to ensure that they are who they claim to be, how it uses encryption to protect personal information and how it's prepared to handle cybersecurity incidents as they arise.

Fourth, the audit would have to describe how the business follows its own policies and procedures. Something in writing isn't worth much if the people who are responsible for implement aren't aware of it or aren't following them. So the audit would have to look into this too.

Fifth, the audit would have to describe the gaps in weaknesses in the cybersecurity program and how the business plans to address them, including the resources the business is allocated to do so, and a timeframe for resolving them.

Sixth, the audit would have to include a description or sample copy of data breach notifications that were sent to consumers or agencies, as well as related information and fixes for the gaps and weaknesses that permitted breach in the first instant.

Seven, the audit would have to include the dates of when the cybersecurity program was reviewed and presented to the most senior individuals in the business responsible for cybersecurity.

And finally, the audit would have to include the certification both from the auditor and the business that the audit was in fact independent and unbiased and not subject to any influence or attempted influence by the business.

Okay. Now they have a sense of who would be responsible for what and what the audit itself would have to include. Let's talk about when all this has to be done. Much like with risk assessments, a business would have 24 months from the effective date of the regulation to complete its first cybersecurity audit. After a business completes the first audit, it would then have to complete the cybersecurity audit and submit its certification annually, in other words, every year thereafter. There also cannot be a gap in any of the month covered by successive audits.

One final point we'll make regarding cybersecurity audits is much like with risk assessments, there's no requirement that a business complete a duplicate audit. So if a business has completed a cybersecurity audit assessment or evaluation for some other purpose, and what it has done already meets the requirements in our draft regulations, the business would not be required to redo that same work for the CCPA. It would have to add to that what it had already done as needed, however.

So if the audit assessment or evaluation needed for some other purpose did not meet all the requirements, the business would've to add to that to meet -- to make sure that it meets all the ones in our draft regulations. Now I'll pass back over to Phil.

MR. LAIRD: All right. We're almost there. We've

hit you with a lot I know. But I appreciate my colleagues giving that really helpful overview. And again, this was mentioned before, if you haven't already got one, there are fact sheets on each of these proposed regulations in the back that I think give a helpful overview of what we've been presenting today. And these materials are all available on our website as well.

So briefly, now I'm going to go over the formal rulemaking process. The agency is sort of on the precipice of starting but we haven't -- we're not there yet. So I'll take you to the next slide. But there we go. So rulemaking in California for a California State Department or Agency has three basic steps. So step one and where we are as of today is that we are refining draft regulatory text based upon the Board's feedback at its March meeting.

That's right. The -- our agency Board has considered these regulations in their current form at their most recent meeting and have directed staff to go ahead and prepare the formal documentation to start that formal rulemaking process. But before step two can begin, the Board will be receiving and hearing once again that full package of documents to review, and we'll have to make a vote and make that decision of whether or not to actually start the formal rulemaking process for the agency or further work on these regulation texts some more. But as

was mentioned earlier on the law does actually require we promulgate regulations on these subjects. So in one form or another, regulations will be eventually arriving on these topics.

After these documents are prepared though, and if the Board does vote to send them to formal rulemaking, then the next step is that formal rulemaking would begin. And it begins when these package of documents is filed with a thing called the Office of Administrative Law. And importantly, that starts what is a typically a 45-day public comment period.

The public comment will be -- can be received in a number of ways. It can be received in writing to the agency. And also the agency will be hosting a public hearing, not totally unlike this one although potentially virtually where we would receive oral comments as well as written comments.

After the public has provided those comments, the agency considers those and responds to them. Now, this can't be a time intensive process. In fact, the law does require us to respond to every comment received during that public comment period. But not only will staff review and consider those comments, but the Board will as well. And that the Board at that point would consider the extent to which it will either adopt the regulations as drafted or

further modify the regulations in response to public comments.

If the agency substantively revises the proposed regulations after that 45-day period rest assured any modifications would actually then go out for yet another public comment period. So there will be robust opportunities for public comment and input on these, especially on any changes. Those comment periods are typically 15 days instead, but again, would be another opportunity for the public to provide feedback, especially on those parts of the text that are changing, for instance, from what you've seen today.

And once the agency reviews and responds to all public comments, and once the Board determines that they have finally gotten the text right, they would vote to adopt the regulations and send them to the Office of Administrative Law and Entity separate of us for final review and approval. And that's step three. So step three is that the Office of Administrative Law will consider the rulemaking package, and then it has 30 working days to make a determination of whether or not we've complied with all aspects of the Administrative Procedures Act. And if so, then the regulations would go into effect.

Okay. Yes, that's right. And what does the agency need to do to -- let's see. Sorry, apologies. So

now finally, a few tips in terms of submitting public comment. Obviously, you're all here today, that's wonderful, and we'd love to hear any feedback really you have today. But as we move into the formal rulemaking period, and we understand some people may be preparing written comments for those first of all, we always encourage people to subscribe to our e-mail list to receive updates on rulemaking. So, you know, for instance, when we're in that 45-day public comment period. And not only can you get those subscribe links and opportunities on our website, but I believe there's a signup page in the back of the room today as well.

You can also attend our Board meetings. They're all open to the public and our public hearings as well. And these are always posted on our website at least 10 days in advance, as well as you can watch recordings of our past meetings. And finally, you can submit public comments during our formal rulemaking. We have included a link here for the tips on submitting effective comments.

So at this point, that kind of covers everything we plan to cover today. And now we'd really like to switch the format around and turn to all of you. And we really welcome this time for any comments from the group. I might hand it over to Megan who I think is going to moderate that component of today.

MS. WHITE: Yeah. Is that going to like, so you would like provide public comment as I mentioned earlier, feel free to come up to this podium. I'll be timing you from right here. As I said, I'll give you the little one minute left signal and you'll be hearing a ding when it's time to grab up five minutes for public comment.

MR. LAIRD: And I'll just mention, you know, at this point, staff really is going to be in listening mode. So we may not be able to be in a position to, you know, directly respond if there's open questions in a comment. But we are listening and if there's anything we can clarify today, we will. Otherwise, they -- everything is certainly being -- we're taking careful notes and we're really paying close attention to everything being said and asked in these sessions. So thanks in advance.

MR. PEREZ: I did not become an -- a business person. I did not become a lawyer. Society needs those things. They need you. I became an artist and I would like to think society needs artists as well. So I know these policies that cover all different types of businesses. And so a lot of these terms are general. And so while I'm sitting here, I'm thinking, well, when they say data, you know, when does that include art? You know, I see photos mentioned people's faces. I wonder when does that include pictures, drawings of people you know, things that are close

to photos, but not quite.

So I did prepare a a statement here. I'm Zach Perez and I'm a professional artist in the movie business here in LA. Our livelihood depends on our being paid for the artwork we create. However, our work is being stolen directly off of our computers by the very drawing programs and creative services that we need to use for work. Beautiful, highly sophisticated images are being easily created with AI by anybody who can really type a sentence.

The images are so beautiful and sophisticated because they recombine millions of pieces of art made by myself and my peers. Worse, much of the art we create under NDAs, non-disclosure agreements, containing and depicting designs and sensitive data ultimately worth millions of dollars. All of this is whisked away to be processed by AI on the Cloud with or without our knowledge, our consent to threaten reemergence and potentially infinite iterations by others. We are being forced to compete with forgeries of our own work, and we cannot, we are already losing work and many are suffering and leaving the business. New waves of young people are being turned away from careers in art like never before. Or almost worse, they're being rerouted to become AI prompters instead of artists.

Indeed, in an age where technology allows artists to create more and more mesmerizing pieces of art,

technology is now being used to replace the artist themselves. People can type 'in the style of' this artist or that artist and get art that looks like the artist drew it because hundreds of thousands of art from that artist were laundered to create the forgery, a deep fake of an original as if it was made by them.

The trade dress of countless artists is offered up for essentially free to be used at will. The thought of infinitely free art seems appealing, just like infinitely free music seems appealing, but the result is the same. It requires that our data and our livelihoods are stolen. And that's the end of my formal statement.

And just in general, from like, what I'm picking up here, which by the way, like these terms for me is like maybe some of you handling a paintbrush, like my brain is like trying to wrestle with them, you know. But what I'm picking up is it seems like like the image -- the AI companies, they might have to do the cybersecurity risk assessment and, you know, they're going to have to look at the images and data that people are uploading to their services. And they're -- I feel like they're going to find tons and tons of risk and violations of people's copyright and identity and privacy. Because that's exactly what's motivating people to do it now, is because they can upload anything they want and then pull anything out of it and

pretend like it came out of nowhere. But what went up into it is all of our -- all of our data, all of our private creations, our faces, our pic, you know, photos and art gets used alike, indiscriminately.

And ADMT decision making, I'm a storyBoard artist and some of my peers are concept artists in the -- in the -- in the industry. And the reason we're employed is because the images that we are creating, the movie executives, the directors, the producers, they're using our images to make decisions on how to shoot the movies, how to budget. They are making decisions based on the art that we're providing. So if the art we're providing is replaced with images that are generated by AI, then they are -- I think ADMT starts to potentially come into to play at some point, arguably. But I think there's an argument there.

And that's the summary of what I have to say. Thank you for listening. Thank you for what you do. This agency is fantastic to see we live in a new age and we need to create new things and think in new ways. And some people see that as innovation. And I love innovation. I'm a futurist. I want the future to be here, but I want the good future. I don't want the bad future. So we have -- we have to make sure that we're working toward a good future. And thank you very much.

MR. LAIRD: Thank you.

MS. PEREZ: Hello, my name is Noemi Lujan Perez and I'm the president and CEO of ECODiversity. Today, I'm actually here on behalf of the California Hispanic Chamber of Commerce, California African-American Chamber of Commerce, CalAsian Chamber of Commerce in (inaudible) Institute. These chambers collectively and individually represent protected categories and under Title VII, the protected categories you mentioned during your presentation.

Based on the 2023 report from the California's Office of the Small Business Advocate, CalOSBA, we can tell you that if California's minority owned small businesses were a State, we'd have an annual GDP that exceeds the GDP in 18 of the 50 US states. Minority owned businesses account for 45 percent of the small businesses in California, that's nearly 1.9 million establishments based on 2019 census data. We're not making this up. The largest concentration of minority owned businesses or minority business enterprises are in LA County. Thank you for coming to us. The San Joaquin Valley, Kern County, and areas which include Merced, and the Stanislaus County.

The business sector with the highest concentration of minority owned businesses in California is in trade transferred and utilities. This includes wholesale trade, retail, trade, transportation, and warehousing, as well as utilities. Many of these businesses, by the way, have

transitioned into AI. My message on behalf of the Minority Business Enterprise Collective is do not let AI become the new digital divide. We are collectively concerned that MBEs are not being reached in to for public awareness.

We are concerned about the lack of MBE or Minority Business Enterprise voices in addressing concerns and or shaping privacy regulations and their impacts on our respective businesses. We are collectively concerned about the disparate impact that privacy regulations may have on MBEs as well as job seekers. We are collectively concerned about the disparate impact of profiling on communities of color overall. We are concerned about the compliance impact on MBEs. There is a lot that you shared today.

We're concerned about attempts to replace diverse talent with AI. The gentleman just mentioned the impact on the creative industry. Well, we are concerned on the impact of replacing diverse talent. AI cannot replace DEI. We want to ensure that MBEs are part of the supplier diversity and remain so, and remain protected in the regulations that the body considers. Beyond the stakeholder meetings and public comment process whenever it starts, we encourage the CPPA to formally engage with the here mentioned chambers, not just for in reach and awareness, but just in the training aspect of everything you mentioned. Again, we do not want AI to be the new digital divide.

Most of the AI technology that is implemented by MBEs tends to be around AI and marketing strategies. It allows for smarter allocation of resources, ensuring that MBEs can reach the right consumers with the right message at the right time, et cetera. But again, we're afraid and concerned and we want to mitigate our own legal issues with compliance with HR law issues on the process. So please engage the hearing chambers. Thank you.

MS. TONSAGER: Hello, I'm Lindsey Tonsager. I'm a partner at Covington & Burling, and I'm speaking today on behalf of the California Chamber of Cumbers. CalChamber represents over 14,000 member companies, the vast majority of which are small businesses. CalChamber raises four concerns with the draft regulations today.

First, the draft regulations are out of step with where the California legislature and Governor Newsom are on these same issues. A 2022 bill regulating automated decision systems in the employment context was never voted out of committee. Yet the draft regulations would impose requirements abandoned by the legislature. And approximately 30 different consumer AI bills are currently under consideration some of which address the same issues covered under the draft regulations.

The draft regulations also risk undermining the goals of Governor Newsom's executive order on AI, which

empowers certain agencies to engage in a formal process with the legislature to develop policy recommendations for responsible use of AI. Governor Newsom recognized that a measured approach is needed for California to both shape the future of AI regulation as well as remain the world's AI leader.

The draft regulations threaten this delicate balance and risk creating inconsistencies with the initiatives launched under the executive order. The Agency should not get ahead of the legislature and the governor on these important issues.

Second, the draft regulations exceed the limits of the Agency's authority under the CCPA and our intention with constitutional principles. For example, the law authorizes the Agency to regulate automated decision making only in the limited areas of opt-outs and access requests. However, the draft regulations go beyond this grant of authority by imposing AI requirements across a broad range of additional topics.

Furthermore, regulating the use of ADMT in publicly accessible places is at odds with the laws carve out of publicly available information and is inconsistent with constitutional principles and judicial holdings. The individuals have no reasonable expectation of privacy in public spaces.

Likewise, an unprecedented opt-out for a new category of advertising also is incompatible with the text of the law. The CCPA requires an opt-out only for cross context behavioral advertising. A term that is defined in the law and like other state privacy laws, is intended to permit unrestricted use of first party data for advertising.

The draft regulation in effect, rewrites the law by expanding the scope of the advertising optout and a new right to opt-out of having personal information used to train ADMT goes beyond the law's definition of profiling. The regulations must be bound by the law's definitions.

Third, the draft regulations are inconsistent with other state and federal privacy frameworks. The draft regulations place many businesses in a perpetual state of conducting cybersecurity audits and privacy assessments. Paperwork and red tape that diverts critical resources away from the hard work of actually building resilience and defending systems.

It also runs counter to the White House's National Cybersecurity Strategy, which calls instead for regulations that minimize the cost and burden of compliance. Instead, the regulations should follow other state's leads in coalescing around the use of generally accepted cyber frameworks and privacy assessments based on consistent standards.

Fourth, the draft regulations are not narrowly tailored to risks of consumer harm. As drafted, the regulations include vague standards that are difficult to apply in practice. For example, CalChamber agrees with Board member Mactaggart that the definition of ADMT is overly broad and should be narrowed.

Similarly, requiring a risk assessment whenever AI or ADMT is capable of being used for the specified purposes, even if the business will not actually use it for such purposes. Risk stifling socially beneficial uses of AI and ADMT with no corresponding benefit for consumers.

For these reasons, CalChamber asked the Agency to revise the draft regulations so that they are consistent with and harmonized across existing laws to defer to the legislature and governor on any overlapping policy issues and to base the regulations on actual risks of consumer harm. CalChamber appreciates the opportunity to provide these initial comments and will elaborate on each of these points as part of the formal rulemaking process. Thank you.

MR. LOWE: Good afternoon. My name's Albert Lowe. And first, thank you for the opportunity for hearing from the public. I've been in the labor movement for 25 years, and I currently work for the UFCW Local 770. And we represent 30,000 food retail, drug retail, pharmacists, lab scientists, cannabis workers, and meat packing workers in LA

County, Ventura County, Santa Barbara County, San Luis Obispo County, and Kern County.

AI and technology are some of the trendiest parts of food retail. The largest food retail companies in the US, namely Kroger and Albertsons, are obsessed with tech. In this period of late capital, food retail is more concerned about partnering with tech than providing good jobs and good customer service. I mean, they spend more on acquiring companies, but I mentioned late capital like that instead of actually producing or creating jobs.

Their business is as a data collector is equally as important as being a food reseller. Kroger and Albertsons uses AI fulfillment centers, basically warehouses where automated carts restricts food items for delivery and continue to collect data and metadata on sales and customers. Now, there are rumors about what these companies also do with facial recognition, but because I don't have any proof of that, I'm not going to address that. But I will address some of those they do in tech.

We're all familiar with the self checkout and all those crazy stories that come along with it. Whether I -- it asks you to tick which -- outrageously to a machine, right? Or you know, how the machine never worked properly. They always need to go back and get some of this help and then you have now three machines that only one works, right?

I'm not here to go over that. What I want to go over a little about what are more side effects of some of these self checkouts.

One, there's fewer staff in the stores. Staff feeling unsafe due to -- because there're -- there's fewer of them. Abandoned carts full of items because of customers just giving up. Fewer staff to address customer concerns, empty shelves and inventory on the -- on blowing docks. To make them employee and shopper experience more enjoyable and safer, food retail should invest more in the staff in conjunction with smart technology.

So our members have been working in food retail for decades. They know how to improve the worker and customer experience. Their voices should be included in the ways technology can improve the company especially when it comes to staffing. There's a sweet spot in staff, I'm sure you -- I'm not even know it -- business knows this, where it to optimize your profits, you want to reach a certain point in staffing.

If you do a little bit too much, you waste -- you've used more on labor. And you go too little, you -- the work experience and customer experience is weakened. So instead of turning checkout aisles into self-checkout registers and how to -- and how to reduce the first mile, last mile Kroger and Alberton use technology on how to

reduce food waste, which is there is a lot of, or how to follow certain laws to also get passed like the -- their work week, which is passed last year in the City of Los Angeles. They can easily use these tech for those reasons before reducing staff.

Increasing staff is the number one way to reduce staff and promote safety. Our members have told us many times that more staff make them feel safer. And especially in light of these like violent staffs or crimes that's taken place that represent under media all the time because they -- our workers see that and they see the solution is more staff not better technology.

Some business pundits, I mean, argue that increased staffing improves the customer experience, reduces theft, improves safety, and reduces staff turnover. So in closing, what I want to say is it -- we're not -- unions are not anti-tech, but the stakeholders need to be brought in these conversations when tech is used. And like I said, our workers know their work really well and can know -- they know how tech can support both their own jobs as well as customer experience. Thanks again.

MR. YOUNG: Sorry I'm a little bit nervous. Hi, my name is Andrew Druly Young. I am an artist working in film for the last 20 years. I'm very happy with my career. What I do in California is not unlike what a lot of Californians

actually do. A lot of people admit that what I do represents a significant part of the California economy, specifically working in the entertainment industry. Why I'm bringing this up is specifically, as an artist who's been doing this for over 25 years, I am constantly at the forefront of technology and I'm always working with it -- place in technology, which is why I've been able to do this for the last 25 years.

That being said, never has this ever been happening before within the last five years, where the very software that I'm using, being specifically Adobe Photoshop, you know, Google and whatever has started spying on me and using my own work against me, literally using my data and training it so that eventually I could be replaced by itself.

This is very hostile to the actual consumer, me, using this actual software. So that being said, I actually think contrary to what a lot of people think is, I don't think the CPPA regulates enough. In fact, I think the CPPA needs to be -- you guys are the only thing that's that's keeping us safe quite honestly, because I know I -- although I'm very Protech, I'm very ProAI in certain respects for tools, I really do think ADMT and AI is at contrary -- is at odds with humanity itself because its own intention is to replace humanity.

So that being said after listening to the rules that you guys have proposed, I have a few notes that I think will be very helpful. One is that opt-out should be on by default. It should not be opt-in. You should not automatically be opted in to anything, and then you choose to opt-out. Opt-out should be the first option and if you want to be part of giving them training data, you should be able to choose to do so.

A lot of these companies -- a lot of the software companies, a lot of these things that involve AI or automatic-- ADMT, they usually make you -- you're automatically opted in as soon as you're part of it. You don't -- and they hide where you can opt-out. You -- it should be the other way around. You should already be -- opt-out should be the default position.

Second thing, you guys brought up a really great example of the human reviewer needs to be available if you choose to opt-out. I also want to add that the human reviewer needs to be able to be available immediately. Because a lot of times, just because you need to provide a human reviewer, a company could just decide it as like, oh, well, we can make a decision a month from now or two months from now, whatever. It needs to be immediate and effective.

The other question too is what are the penalties for not complying? You know, are these penalties

significant enough that is actually going to provide safety for us? For example, these penalties need to be significant enough that it's not just another tax for a company to play with -- to pay with. Because just for example, like parking in Los Angeles, everyone knows that parking in Los Angeles is extremely difficult. And sometimes, yes, if you park in the wrong spot, you pay a $200 fine.

Well, for some people, for certain peoples of a certain social class that $200 fine is just premium parking. So what I'm trying to prove is that a lot of these billion dollar companies, especially if you look at the AI companies, these penalties need to be significant enough that it actually affects them in such a way that they actually pay attention. It's not just another fee for them to pay.

The -- also 24 months to comply is too short, quite honestly. And the last two years alone, Chat GPT itself -- actually two hours ago, Chat GPT just released a new software called Chat GPTO, two hours ago, where first time forever -- first time in a long time that we actually have AI that actually sounds like a human being that's collecting our data, that's actually fully aware and very much this is be opening up to the public where everyone's going to be spied on constantly and our data is going to be freely just being taken.

This is very dangerous for people like me who also have diabetes. What if I'm on the phone with my doctor and I'm not -- I'm -- I don't know there's a machine listening on me. Someone could come by and ask that machine, hey, what was Druly Young talking about? And that machine will freely break that privacy and tell them what was the conversation I was having. Just because this machine is always constantly listening, no matter what.

What do we do about opting out then? Is there a way to -- can -- is there any kind of indication that we know that we're being -- you know, we're being opted in to or opt-out. We don't have an option where it's openly and public that way. So I -- in my opinion, it should be shortened to 12 months. It should be sooner than that because the rate of innovation is just too quick. 24 months is just too long. That is practically a decade to a lot of these companies that don't care about humanity at all whatsoever.

And lastly, I do like the idea that you should have a smart auditor looking over the systems. However, an auditor working for the company, isn't that in conflict of interest? I'd like to bring up a recent example of what happened with Boeing, specifically, with all the planes. They had used internal auditors, and that led to the failure of the planes at Boeing. Clearly internal auditing doesn't

work. Thank you very much. I really appreciate you guys for holding this session.

MS. KEEFER: Hi everyone, my name is Tasia Keefer. I'm here on behalf of the LA County Business Federation, also known as BizFed. We represent over 410,000 employers and 5 million employees throughout LA -- throughout Southern California, excuse me. And we represent not only Chambers of Commerce and minority businesses, but also industries that will be impacted by your guys' decisions.

We thank you for hosting a stakeholder session here in LA today and allowing us to provide public comment today. But you should be aware that business organizations and individual businesses are completely unaware of the risk assessment and automated decision making mandates and requirements that you are proposing. We do not know what problems that CPPA is intending to address and whether those are legitimate problems that justify a new regulatory program.

And we are concerned that proposing these regulations will create costs at a time when business costs, wage increases and economic uncertainty threaten Southern California businesses. We respectfully request that the CPPA engage in a real effort to inform Californians about the regulations that you are proposing. By engaging with business sectors such as entertainment, goods movement, and

manufacturing.

The population of Southern California exceeds 24 million people. A single three hour session is not enough to engage the public on this issue and to provide valuable input. Some of our initial thoughts are the CPPA's draft regulations have a significant impact on California's diverse sectors and communities. In LA our membership is leveraging AI and Automated Decision-making Technologies in all -- in all sectors.

Our members' use of ADMT greatly differs from that of Central Valley or Northern California, and we're concerned that the draft rules do not consider the unique regional and sectoral applications of this technology. Instead, the proposed rules use an overly broad definition that forces practically all businesses to comply with the new risk assessment obligations.

The draft rules also create a new opt-out mechanism that would break basic website functionalities that businesses rely on to improve their customer service, such as recommending similar items, preventing fraud, and performing basic A/B testing and analysis for improving website functionality for consumers. These simple low risk uses of ADMT are critical functions to help businesses improve customer service, manage inventory, and ultimately drive revenue. Therefore, we urge the CPA -- CPPA, excuse

me, to offer a narrow definition of ADMT.

There are many benefits enabled by artificial and automated decision making for our businesses, but also the community. You may have seen that the Homelessness Prevention Program that harness the power of predictive AI to identify individuals and families who are at most risk of becoming homeless, which then allows the county to step to offer aid to them, and then get stabilized and remain housed. This program has helped serve nearly 800 individuals and families at risk of becoming homeless.

These use cases uplift both the community and local businesses, and we need to ensure that we -- that we persevere -- that we preserve, excuse me, the use of ADMT, and we urge you to avoid regulations that would hinder AI innovation like this.

Lastly, as it relates to how various regions use AI, we recently signed on to a letter last week that -- submitted last week that urges the staff to consider additional stakeholder sessions. While we're grateful to have a meeting like this in our region, there are many stakeholders across the state that should also have the opportunity to have their voices heard. We hope that you'll consider hosting several more meetings that are accessible to both on -- to online and in person, and if they are in person to have the live streaming component as well. Thank

you guys for your time.

MS. GUILLOT: Hello, my name is Elizabeth Guillot. I'm the lead for state and local policy at CrowdStrike. CrowdStrike is a global cybersecurity leader that leverages cloud scale AI to offer real-time protection and visibility across the enterprise, preventing attacks on endpoints on and off the network. Given that I work for a cybersecurity company, my comments will be focused on the cybersecurity audit part of this regulatory process.

Firstly, I think it's great that the CPPA is wanting to improve cybersecurity across the state. Cybersecurity adversaries are growing more sophisticated, their attacks are getting more severe, and they target a wide variety of sectors. This can be from the agencies themselves to small and medium sized businesses, and really everything in between. And these trends are only growing more severe. The number of attacks we see each year are growing along with the number of adversaries who are actually carrying out these attacks. So while I said it's great that you guys are looking at this issue, I do want to point out some of the limitations of a cybersecurity audit as a cybersecurity tool.

They are very useful tool for an organization to capture a snapshot of the existence of cybersecurity plans, strategies, and controls. However, these are just that a

snapshot in time. They cannot reflect a real time measure of the state or an organization's cybersecurity practice. Since we recognize that you are proceeding with auditing scheme, I would caution organizations who fall under this to be overly reliant on the results. Just because you have a successful audit doesn't mean that your cybersecurity landscape can't change in an instant. You know, one mouse step from an employee, one link that you click on and you know, your whole landscape has changed momentarily.

In addition to a cybersecurity audit, there are some cybersecurity best practices that entities covered under these new regulatory should consider deploying and these can help reduce the risk of data breaches or a cyber attack. Some of these technologies that we often recommend to customers and clients include endpoint detection and response, identity protection and authentication, logging practices, threat hunting, machine-based learning prevention, and considering managed services providers.

One technology that I already saw noted in the slides this afternoon was multifactor authentication. That is a great first step for organizations to take. However, the next iteration of that in a more principle based approach would be deploying a zero check -- a zero trust architecture. Due to fundamental problems with today's widely used authentication architectures, organizations must

incorporate new cybersecurity protections that focus purely on authentication.

A zero trust design would radically reduce and improve lateral movement within an organization. So that way if an adversary does get access into, you know, your network, they're segmented and aren't able to have free reign within your networks where -- aren't able to get into even more sensitive information. So a zero trust architecture does incorporate multifactor authentication. However, it also uses other tools, keeping this zero trust mindset to keep, you know, a potential bad actor from moving around within your network. So this can also include logging, endpoint detection response, next generation firewalls. It's more taking a mindset to the security rather than just having MFA on its own.

My final point is that with these certifications that you guys mentioned throughout the day, both for the cybersecurity audit and for the risk assessments that details about these, do not become public making detailed cybersecurity audit or a risk assessment results public could hand those bad guys the keys they need to target the very organizations that this regulation is trying to protect. So it sounds like that's not -- that wasn't presented today, but would just urge that not to be the case. Thank you again for your time and I look forward to

engaging with you all further within this process.

MR. ROSS: Good afternoon. My name's Tom Ross. I'm with the -- I'm a board member of the United Chambers of Commerce on their government affairs committee and a member of the San Fernando City Chamber of Commerce. And by extension on the crowd chambers, I was in Sacramento with them last week. And one of our first issues was basically, as others have echoed the fact that this is -- seems to be under the radar.

While we are a very involved group in the San Fernando Valley with a large contingent of small businesses, this only came across our desk several days ago, and I'm the substitute guy. The usual guys aren't here. So, you know, I got my little talking points, but I'm going to skip those because of the timer over there. The issue for us is if you're going to proceed with this, let somebody know. Three meetings doesn't constitute phase one by any stretch of the imagination, considering the fact that almost every single business -- oh, that's the other point.

So is there a threshold besides 50,000 contact points? Because I know a dry cleaner who might have 50,000 people on an e-mail list and there's two guys working there and they may make, you know, $8,000 a month. Are they required to file these kind of -- and go through these kind of regulatory, you know, issues because they have a mailing

chimp. What -- where does this end, so to speak, when it comes -- when it trickles down to the largest contingent of businesses? I'm -- let's see here. I had another note here and I can't remember what it is.

Oh yeah, I have a big argument with the fact that you guys are even doing this. You're an Agency that's supposed to affect the -- or manage the regulations that are brought down and not actually come up with new ones. As noted earlier, there's a lot of stuff cruising through Sacramento right now that deals with this exact thing which brings to the point that what kind of carrots and sticks are you going to put into effect? If in fact you are going to go through with this, are you going to provide penalties and are those penalties going to be enforceable by you guys and is it okay? How much is it going to cost me if I don't comply if I'm a small business?

I run an internet service provider. I have very large footprint, but I only have seven employees. So am I going to be under the same kind of scrutiny and I already comply with a whole lot of things because I don't -- my lawyer doesn't want me to be liable for things that I shouldn't be. But that's because I'm a prudent businessman. That's what I do. And that is the responsibility, and that's what Chamber of Commerce's teach to their small businesses, is to be responsible.

Now, I know a lot about AI and I'm not really worried about it. What I'm worried about is this, which is a reactionary set of regulations that may or may not come down that are without representation from those I voted for and those I lobbied last week on issues similar to this. So I think it might be more productive if we focused on software developers whose responsibility is to develop the software that I'm going to buy, and I'm not going to buy it unless it already complies. So shouldn't they comply, not me.

So for example, we -- you know, in our dry cleaner scenario, he should be buying, you know, QuickBooks/ MailChimp, which already complies with those things you're talking about, which is a nationwide software company, which is global in reach, which may have to comply anyway. So why do we have to have another set of regulations that I've got to deal with as a small business or other small businesses within the realm, so to speak.

Let's see. And what other regulatory issues are already in place that this piles on top of and why? I really would like to know what compels us to do this in light of the fact that a lot of these things that we're talking about are in flux. Does everybody still understand that we can't spit on the sidewalk in San Francisco even though that law was passed 150 years ago? Does it matter

anymore? No one chews tobacco. Things change very rapidly and as was already noted, Chat GPT is not finished. Most AI isn't finished. And most people haven't implemented it in a meaningful way.

So we are restricting technology development by restricting how it can be used without even understanding where it may end when it's done. There are already people with tools available to scan the databases that are used to train things like Chat GPT so that we can see whose copyrighted materials in there. So do we need a regulation or is it already part of the deal? So that's all I can do in my three minutes allocated. Thank you very much.

MS. WALKER: Hello, I'm Kristen Walker, Professor of Marketing and MBA Director at Cal State University, Northridge. I come to you today after studying privacy since 2010, back with FTC before they started the Privacy Con, which I appreciate. First of all, I really appreciate what you guys are trying to do. I commend the fact that this Agency has been created, and I think that you have a very challenging job ahead of you. I don't envy it. And anytime you're creating policies I think all of you know, it's going to be very challenging to have a one size fits all, right.

So I have some questions today, and then I have one industry based on my research that I kind of want to

highlight for you and your focus. And I offer my assistance if you need it, and I'll participate in public comments as we go on. I concurr with some of the comments here that, you know, my research, especially on consumers surrendering data, not sharing data, really says that access and opt-out choices for consumers after data is collected is kind of a moot point, right? That means that they've already surrendered that data.

So that's concerning to me, and it's somewhat awkward. But, now that we're here, I think the one thing that I have with the ADMT and the risk assessment, the question that I have is 24 months to submit to CPPA. I think it would be helpful to understand the rationale for that two years. I'm concerned with large companies, not small businesses, and large companies are very nimble. They should be able to do this risk assessment very quickly. And two years is an awful lot of problems and consumer protection issues, in my opinion.

So I'd really like to see why two years for that. I think one particular industry is especially concerning for me, based on my research, and that's the ed-tech industry. My research shows it's problematic for a vulnerable population, children. And I am very concerned about this, and I'll give you a personal antidote. I opted out for my daughter who's now her second year at Berkeley in college.

I opted out when she was a freshman in high school for Naviance, that college sort of tracking tool, and it didn't matter. She was still a part of it. So that opt-out didn't work. I was probably the only one that opted out at the time, but still, right?

So I'm really concerned about the guardrails on this industry, especially because this industry is really operates in the shadows. It's part of larger tech companies. It is a hundreds of billion dollar industry. And in my research with California schools, I really -- we found a privacy security chasm where the schools are really concerned about keeping the data of children safe, but -- and they're relying on companies to keep the data safe, but that data can be co-mingled. And as we all know, clouds only exist when you look up in the sky.

Otherwise, it's a data center, right? So I really want to make sure that you guys are focused on that industry in particular because I really find that it's a growing concern and there's no eyes on it right now. So thank you very much. Best of luck.

MR. PLANK: Hello, my name is Manuel Plank. This is the first time I'm doing this, actually, so I'm also very nervous. I am an illustrator slash concept designer in the movie industry. I've been doing this for 25 years, just like Mr. Laris and Mr. Leon. And as said before, I think

what's really important is with the new AI technology and the software subscriptions that we're using, that actually should be more regulation than less regulation, because -- and as he said before, as mentioned before that the opt-out option should actually be the default option because all the work that we create now using software packages, a multitude of 3D programs, painting programs, image editing programs -- we don't have a choice if the work that we create or whatever is on Google right now is being used to train AI, to replace us or to forge our work because my artistic style or our artistic style, how we create images is also linked to our name.

And so our creative identity is very important for our professional reputation or for our social reputation for that matter, because it's linked, because we have an online presence with our images to promote our work. And also, as was mentioned before with regards to NDAs. So with our data being collected by the software companies it is easy now to then forge images that look like actually it's been created by me or by my peers. So for example, if you work on a movie, you sign the NDA and you cannot publish your images until the movie's been released, or you got permission by the movie studio, the production company.

If somebody knows, and you can track people's names online and find out if they're working on a particular

movie or on a video game project or whatever creative endeavor that might be you could create an image that looks like -- just like my work, and pretend you have an image that I did to create traffic for your own website or social media channel or whatever, and make money off that. And that would actually get me into legal trouble because it would look like I violated the NDA, even though I never produced any of this artwork.

And the thing with that is also before -- when I started 25 years ago, I was like, of course, I created all the artwork with traditional means, pencil, paper, paint, paint brush. And then you use and embrace new technology like 3D software, painting software, image editing software. So you adapt and you create your art with new technological means. But these software companies moving into AI territory now are using what we are producing actually to replace us and also enable people that never adapted to any creative challenge or change to do what we do.

So I don't know if that makes any sense. In terms of they -- before it was much, much harder to fake something that we produced. A forgery before would require a certain degree of talent and of course, training and years of experience. And now with us giving basically, or being forced to give our work to these software companies or our work being on Google or wherever on any internet platform,

it gives people actually very easy without any or very minimal means to fake our work. So that's basically all I wanted to say. Thank you very much. Thank you.

MR. KAMAL: Hi, my name is Sop Kamal (phonetic) my first time here. Thank you for all the comments, that feedback some of the -- some of the folks here has provided great stuff. And I actually love the opt-out by default suggestions that one of the folks here had as well. I think that's a -- that's a great idea. Because I have some general questions. I just want to pose the greater audience here is in terms of privacy, right.

There's CCPA, there's very other 15 plus states in the United States that's issuing their own versions. And now there's something called the APRA, then the American Privacy Act as an example, right? That's coming into play, right? In terms of crosswalks, I mean, what makes us more special than relative to some of the other states as well as some of the APRA that may be coming about very shortly, right? Which is still TBD that's still in flight in terms of the privacy discussion. You're in Congress right now, right?

Also in terms of you know, general guidance, right? There's a lot of good examples that you mentioned, right? But from a generality perspective, are any -- are there any specific guidances that we as practitioners could

potentially leverage in terms of following, you know, NIST CSF -- NIST, you know 853 or NIST privacy as an example. The reason I'm bringing this up as an example is that Tennessee they just recently I guess approved their privacy cadence, right? And one of the things they said was, if you're leveraging the NIST privacy framework, right, in terms of best practice, then you should be in decent shape, right?

So from a C -- from a CPPA's perspective, or they general guidance, maybe not now, but sometime in the near future that we may think about, right? In terms of a -- you met -- there were talks about assessments, right? 24 -- was it 24 months at the station and follow up with 12 months, right? So in terms of from a CPPA's perspective, do we have the capabilities to actually triage the submissions of all these assessments and any follow ups, right?

So I was just wondering if there are any of -- any key plans in terms of building up your army, so to speak to -- very similar to the IRS in the event that you want to enforce some of these regulations, right? And if so, what does that look like? Because the small companies here, you might not be, you know, really worried about, but some of the big boys like ed-tech companies, right? They have an army. I mean, I'm not sure if you guys are not have an army or in the process of putting up one. So that was just some

general thoughts that I just had. Thank you.

MS. OWENS: Hello. I hadn't actually planned to do a public comment, but I was coming here to more listen and learn but I just feel compelled since nobody else is talking. My name is Kim Owens. I'm a California native. Grew up in the Bay Area, so I have been in tech my entire career. Started out in tech sales and then moved into tech marketing. And so I've seen decades of iterations of how tech has impacted not only the business community, but the public community.

And in my position as a small business, as a solo entrepreneur I definitely am looking out for the business implications of AI and how that's going to potentially impact me as a person, my business, but also as as a citizen. I've seen how lobbying and the business interests have typically taken precedents because of their power and their money not only here in the State of California, but across the country.

I think that it's really critical that we are having these discussions considering that that AI, many of the AI companies are here in California, especially the Bay Area. But I want to kind of reiterate some of the points that some of the others have made. So I think I also agree tech is moving super fast. OpenAI came out with a -- yet another version, and it's going to continue to move quicker

and quicker.

Google has another announcement, IO developer announcement tomorrow this week on the federal level, they're having discussions about the Create AI Act on a federal level. These are all things I'm trying to stay on top of myself as both a citizen and a business -- solo business person so that I can implement these into my work, but also kind of protect my clients who I'm creating content for. So in the -- in the role of content marketing. And so two years is way too long. It's going to be night and day. We may be at Sentient by then in two years. And so I don't think that's -- I don't think that's logical. I also agree that we need to have more sessions like this.

So I understand that there's a virtual session later this month, which is fantastic. I also as a -- as a certified small business woman-owned business, I saw the a bid come out for an awareness campaign and an advertising level for CPPA. I think it needs to be more broad than just advertising. I think it needs to be education on an ongoing level, not only regarding this actual act itself, but also after it's passed because tech is going to change and regulation is going to have to change with it, both on a state level and a federal level.

I also agree in the opt-out by default. I think that's something that's been recommended on the federal

level by ethical AI advocates. And I also agree that you know, that we need to take both sides into account. I think there was some mention that, you know, the -- some of what's in this regulation is conflicting with other regulations.

So making sure that that's really clear and cohesive is absolutely essential. I -- you know, to support small businesses, a dry cleaner who may be, you know, subject to that -- this type of thing I think is too much of responsibility when they're just trying to run their daily business. So I think the more that the state can do to support them the better. And I think the best way to do that is through ongoing education and awareness. So thank you for all that you're doing for everybody here.

MR. LAIRD: Thank you.

MR. PEREZ: Hello, it's me again. I felt I had to speak because I'm sitting here and the question was just asked, and I know it is 5000 percent figurative and I'm in estate building, so it is a million percent figurative. But the gentleman asked, "do you have an army?" And to me sitting here being in the entertainment industry, I hear -- talk like this all the time and it sounds like corporate bullying.

And I'm a part of the labor movement, I'm part of the Art Director's Guild here in Los Angeles, which is part of (inaudible), which is part of the national labor

movement, which is part of the labor movement, the whole world over which exists purely to combat corporate bullying and the exploitation and theft of our rights. And so I say very figuratively in response to the figurative question, do you have an army? The answer is very figuratively. Yes. Thank you.

MR. ROSS: Just a point of order, I mean, I'm assuming since you guys are going to be here until 7:00, if there's no further public comment, there won't be any interaction or any answers to questions. You're just taking the comment at this point; is that right.

MR. LAIRD: That's correct.

MR. ROSS: Okay. All right. And thank you.

MR. LAIRD: Although I'll take the opportunity to let everybody know on our we've mentioned our website before would encourage our Agency's website is cppa dot ca dot gov, but we also have a website more primarily for consumers, for the public, for businesses, it's privacy dot ca dot gov. And a handful of questions that come up have come up today, I think would be answered on those websites. There's a frequently asked questions portion as well as the resources for businesses about which aspects of our law apply, how do -- how they might apply to your business in certain instances. So again, we're not able to answer, you know, questions directly today, but I would really encourage you

to take a peek at those. I think you'd find some of the resources really illuminating to some of the questions I've heard today.

MR. SOLTANI: I just want to thank folks for coming. We're going to be here until 7:00 Mr. (Inaudible) come after work and this (inaudible) 5:00, so (inaudible) but we're going to all be here until 7:00. You all are welcome to stay with us, but I also -- you're under no obligation (inaudible) so good (inaudible). Really appreciate the comments we will be having as we were set up fully hybrid, in-person and remote option for the -- for the 22nd?.

MR. LAIRD: Yes. Yeah.

MR. SOLTANI: Wednesday the 22nd. So about -- (Inaudible) happened. Yes. Yeah. Sorry about (inaudible). So current tracks to also watch those on Zoom or attend in person What's happening. Thank you guys.

MR. PLANK: Can you say those websites again please.

MR. LAIRD: Yeah. So our Agency's direct website is cppa dot ca dot gov and then the sort of more public facing website is privacy dot ca dot gov.