CALIFORNIA PRIVACY PROTECTION AGENCY BOARD

PRE-RULEMAKING STAKEHOLDER SESSION - FRESNO

AUDIO TRANSCRIPTION OF RECORDED PUBLIC MEETING

WEDNESDAY, MAY 15, 2024

LENGTH: 1:15:49

Transcribed by:

iDepo Reporters
898 North Pacific Coast Highway
Suite 475
El Segundo, California 90245
(323) 393-3768
www.ideporeporters.com

APPEARANCES:

Present: JENNIFER M. URBAN, Chairperson of the Board

PHILIP LAIRD, Meeting Counsel

MARINA FEEHAN, Attorney for CPPA

KRISTEN ANDERSON, Attorney for CPPA

NEELOFER SHAIKH, Attorney for CPPA

MEGAN WHITE, Deputy Director for Public and External Affairs

BRIAN VASQUEZ, Illustrator

ROBERT SINGLETON, Director of Policy and Public Affairs for California and the West US region for Chamber of Progress

BENTON JEW, Illustrator

CHAIR URBAN: My name is Jennifer Urban and I'm the chairperson of the Board of the California Privacy Protection Agency, CPPA. A lot of Cs and lot of Ps in obviously California government just to warn you. But anyway, welcome to this afternoon's panel for making stakeholder session. I'm joined here today by members of the CPPA team to discuss important issues that affect all Californians. Privacy and the use of personal information in Automated Decision-making Technology or ADMT for short. If you haven't had a chance yet, please feel free to take an agenda and handouts, which are located on the check ins table. These are also available on our website, cppa.ca.gov on the meetings and events page.

The agenda will give you a sense of the flow of today's session. The fact sheets are available in English and Spanish, and they provide helpful overview of the topics we're going to discuss today. As you'll see on the agenda after the CPPA team's presentation, which will take about an hour -- an hour, okay? The rest of today's session is dedicated to hearing from you. We are looking forward -- we look forward to listening to your important feedback and answering any questions that we can address at this early stage before the formal rulemaking process.

And I just want to say at the outset there, please forgive us if we can't answer substantive questions and is

for a couple of really important reasons. One, that the rules are still in draft form. They haven't gone into formal rulemaking yet. And so this really is the opportunity to take in information as the rules are being developed. And the other is because the CPPA and the CPP -- CPPA doesn't take positions without the Board voting to do so. And the Board has not voted to take specific positions on the substance of the rules yet because they are in formal rulemaking. So please be patient with us. It's not because we're not taking information at all, we are listening.

The CPPA team will also provide you with more of an overview of the Agency's history and our responsibilities under the law for my little pressy right there. So I'll leave that to them. But just to -- just to very quickly, we are a newer state Agency, I think probably still the newest, established in 2020 by a citizen initiative, the California Privacy Rights Act. As I mentioned, there's a Board that makes decisions for the Agency and it's a five member Board and I'm incredibly honored to serve as the Board chair. I was appointed by Governor Gavin Newsom in March, 2021, and that's when the Board was appointed, that's when the Agency began.

I'm also a Clinical Professor of Law, University of California, Berkeley School of Law and I'm the Director of Policy Initiatives at the Samuelson Law, Technology &

Public Policy Clinic. I served with four other appointees. One person -- another person appointed by the governor, one appointed by the Speaker of the Assembly, one appointed by the President Pro Tempore of the Senate, and one appointed by the Attorney General. I note that in order to point out the fact that all of those five people have to discuss and campaign and vote whether to take the positions, as I mentioned earlier.

So, today we're focusing on rulemaking to implement the law, which is one of the main goals of the Agency and the CPPA Board. As you may be aware, the Agency has been working on these particular free ruling topics for quite some time. We actually started in fall of 2021 with a subcommittee of the Board before we had a full Agency of staff, like now we actually have an Agency. But at that point we only had maybe one or two employees and a subcommittee of the Board began working on these questions of ADMT, Cybersecurity Audit and Risk Assessments.

And as those have been developed over the last couple of years, we are now moving to the next simple steps. A big one is getting feedback from the public and allowing the public to hear more about where we are with these regulations right now. We are really looking forward to hearing your questions and listening to your thoughts. And as I mentioned earlier, we may respond if we can, but our

primary purpose and our primary ability today is to listen. And also to note, we can't give legal advice, which means that we can't answer any specific questions that relates to anyone specific situation.

So, today will be about some presentations so you can learn and then learn from you. And then for next steps, the -- once the staff have taken in all the information from these stakeholder meetings and worked on the regulations some more they will bring them for the Board if its for Board meeting, and should the Board decide at that point to release that for formal rulemaking, then they will go into the formal process.

You will have another opportunity to provide formal comments on the draft regulations once they enter that process and the legal team will have all of this. So I will -- I'll just -- I'll stop like saying things you already going to say. But I'm very happy to introduce the team now. Joining me today are Phil Laird, our general counsel, Neelofer Shaikh, one of our attorneys, Kristen Anderson, another attorney who have been doing incredible work on these really complex issues and on these draft regulations. Marina Feehan is here as well, there she is, another of our attorneys from the legal division and Megan White, our Deputy Director of Public and External Affairs.

Ms. White will go over some housekeeping topics in

just a moment, including how to comment here today. I will just note for now that each member of the public will have five minutes to speak when we get to that portion of the agenda. And if you think of something else that you would like to say or share after today's meeting, we will have another session next week in Sacramento and that will be a hybrid session and so you can Zoom in into that session if you don't want to track to Sacramento but there's -- if you want to -- you want to get further thoughts there. So that would be May 22nd from 2:00 p.m. to 6:00 p.m. and you can find the info for that meeting and the Zoom link for the hybrid meeting on the CPPA website. And with that, I will turn it over to Deputy Director appoint. Thank you, Ms. White.

MS. WHITE: Thank you so much, Chair Urban, and thank you all for joining us here today. Just a couple housekeeping things from me. In the rare case that there is an emergency, we will just file out those doors and right out the front just as you entered. And again, my name's Megan White, apologize, Deputy Director Public and External Affairs. Just to illuminate a little bit on the public comment, as Chair Urban said, everybody will have five minutes to provide public comment. We ask that you come up here to the podium to provide it simply so we can capture your thoughts. Because as you can see, there are cameras

here, we're not live streaming this meeting, but we are recording it so we can record all the public comments that are given today.

This recording will go up on our website, so there's a public record of the meeting because it's a public meeting. If you need restrooms, just head right out the door, you're going to go past the security guard, make a left, and another left, men's and women's are right there. If you didn't have a chance to grab the handouts, feel free we have three different fact sheets. So if you just grabbed one, please note there are three that are available in English and Spanish, and they're also on our website if you didn't happen to grab one or you prefer electronic copy. And last, we have a Spanish translator with her today, Laura, kindly joined us. She's back at that table. If you need translation services, please feel free to see Laura and she'll be happy to assist you. With that, I'm go turn it going to over to our general counsel. Thank you so much.

MR. LAIRD: I thank you all and welcome to our second of three pre-rulemaking stakeholder sessions we're holding across the state. As you've already heard, and you'll hear a few more times, these are -- our purpose is twofold today. First of all, we want to provide information about these draft regulations to a broad population, to more consumers, more businesses, and more practitioners about

what we're doing on these topics of ADMT, Risk Assessments and Cybersecurity Audits. But secondly, we really do want to hear from all of you. We're really happy to have you here and we're excited to get some feedback and learn more about your impressions and reactions to the draft regulations we've prepared.

As the lawyer though, I also have to make the disclaimer. So again, before we get started, I just want to be clear of where we are. First and foremost, I know it's been said once, I'll say it one more time. Anytime we refer to Automated Decision-making Technology, we're just going to say ADMT to hold us -- to save us the mouthful, but that's what we're referring to. But in general, the CCPA, the law we implement here at the Agency, does require us to issue regulations on ADMT, Risk Assessments and Cybersecurity. This is required in the law.

At this point we have drafted those regulations, but we have not started the formal rulemaking process yet. The rulemaking process of California, in fact, has many steps and there will be a number of opportunities for additional public comment. And we will talk about that a little bit later in the presentation. But today, our presentation really is geared towards explaining what the regulations are in the current state and then how you can continue to participate in the rulemaking process. In

addition though, our presentation is not implementing, interpreting -- or interpreting any existing law or regulation, and we are not providing legal advice. If you are a business or consumer seeking to ensure compliance with the law, you should consult the statute regulations currently in effect and your own legal counsel.

Finally, I'll note that any opinions that the three of us end up expressing today are our own and not necessarily those of the Agency, its Board, or any individual Board member. We're here as attorneys for the Agency and we really are honored to be working on these very important issues. And again, we are actually are very excited to hear all the feedback we can get from these sessions and from you all.

So, quick overview of our agenda. As you can see from this slide, we're going to be going over a few topics today. First, I'm going to provide a short background on our Agency and the consumer privacy law that we implement and enforce and what we're currently working on. Then we will go over the draft regulations on those three topics I mentioned earlier. And then finally, we will conclude with how you can participate in formal rulemaking when that process kicks off.

Okay, so background on CCPA and current activity. As was mentioned earlier, in privacy and California, there's

a lot of Cs, there's a lot of Ps, I apologize for the acronym Sue. But to give you a brief runway of sort of how we got here today in 2018, the California Consumer Privacy Act was passed the CCPA and went into effect in 2020. It really was the first comprehensive privacy law in the nation, and it gave consumers rights over their personal information that businesses collect about them. It also required businesses to inform consumers about how they collect, use, disclose, and retain personal information.

Then in November, 2020, California's - Californians voted on Proposition 24, the California Privacy Rights Act, or the CPRA, which amended the CCPA. From here on out, though, when I talk about the law, I'll just call it the CCPA, I think that'll be easier for everyone. Those amendments went into effect in 2023 and such that now under the CCPA there are additional privacy protections now for employees, independent contractors and job applicants, which is relatively rare among consumer privacy laws in the US. It also now includes new rights for consumers. The right to correct inaccurate personal information that a business holds on you, the right to limit a business' use and disclosure of their sensitive personal information. And as we'll be discussing in depth today, the right to access information about and to opt out of -- opt out of a business' use of ADMT, which includes profiling. We're

going to explain exactly what we're talking about when we say that.

As an Agency, we actually have a number of tasks that we're working on every day. But if you really want to break it down into three major functions, it is these. It is rulemaking that our Agency and our Board is to issue and implement regulations that further define, explain or implement our -- the law. We also have a charge to promote public awareness, and we also have an auditing and enforcement function that's meant to ensure compliance with the law by businesses. So today we really are leaning into two of those three charges. When we talk -- we want to talk about the rulemaking and the public awareness roles.

We're here today to provide you with an overview of these regulations and then, as I've mentioned a number of times now hear from all of you. And later during formal rulemaking, I should note there will be additional opportunities for public comment but this is the first stage in that effort. So with no further ado, I am going to stop talking. I'm going to turn it over to my esteemed colleagues, Neelofer Shaikh and Kristen Anderson.

MS. SHAIKH: Thank you. Can you all hear me Okay? Thank you. Okay. So on our first topic, we're going to be talking about Automated Decision-making Technology or ADMT for short. As Mr. Laird mentioned, the CCPA directs our

Agency to issue regulations regarding opt out and access rights for consumers such as yourselves relating to business' use of Automated Decision-making Technology. So today we're going to talk a bit more about what ADMT actually is, so what it includes, and what it does not include. We're also going to talk about when a business would need to comply with the proposed requirements for ADMT. Importantly, the requirements that we're going to be talking about would not apply to any use of ADMT, just specific uses that we're going to talk more about. And then lastly, we're going to talk a bit more about what those specific requirements would be for those uses of Automated Decision-making Technology.

So turning now to just the definition. So what is ADMT? As Mr. Laird mentioned, that's a mouthful, and so we're going to break it down into four components. So the first thing, to be ADMT it needs to be a technology that's actually processing personal information. So it's collecting, using, storing, disclosing or otherwise handling your personal information. That's the first part of the definition. It also needs to be using computation, and most importantly, it needs to be using that computation to replace or substantially facilitate human decision-making.

And when we use that term, substantially facilitate, we mean that the output of that technology is

serving as a key factor in a human's decision. So for instance, if you are using a technology that generates a numerical score about a consumer that a human reviewer is using as a primary factor to make a decision about them, that would be a use of ADMT, because that output is substantially facilitating a human decision maker's decision. Lastly, ADMT includes profiling, which I'm going to talk about a bit more on the next slide.

Examples of ADMT include things like resume screening tools that businesses use to decide which applicants they plan to hire. It also includes things like facial recognition technology that a business uses to verify the identity of consumers as they enter, for instance, a workplace. And lastly, it would include tools that place consumers into audience groups to target advertisements to them. Lastly, we just want to note that ADMT does -- generally does not include routinely used technologies. So things like spell check, calculators, spreadsheets are generally excluded from the definition.

Now turning to profiling. So Automated Decision-making Technology includes profiling. So what is that? Generally it's two things. It's -- or it's broken down into two components. So first, there has to be an automated processing of personal information. So automated collection, automated use, and that needs to be done to

actually evaluate a person. So, for instance, to analyze your ability to do or be something, your reliability, your health, your economic situation, your interests, your predispositions, your behavior, your movements the automated processing would need to be evaluating something like this about you to constitute profiling and therefore a use of Automated Decision-making Technology.

So now that we've covered those definitions, it's helpful now to talk about who actually would need to comply with the proposed requirements for ADMT. So first, you would need to be a business under the CCPA. And when we use that term business, it generally refers to a for-profit entity that meets certain additional requirements under the law. So for instance, businesses that make over $28 million in annual revenue would likely fall under it, assuming they meet the other requirements of the statute. And we have a helpful fact sheet available online on our website to help you assess whether you are a business that would need to comply with the CCPA. But assuming you are a business under the statute, you'd also have to be using ADMT in one of three ways for significant decisions, for extensive profiling, and for certain training uses to be subject to the proposed requirements and I'm going to talk a bit more about each of those uses.

So turning to the first use case, the use of

Automated Decision-making Technology for significant decisions. That generally refers to decisions that have important consequences for consumers. So the use of ADMT, for instance, to decide whether to terminate someone from their employment or suspend them, that would be a significant decision and that would be a use of ADMT for a significant decision.

We've included some examples on this slide of different types of significant decisions. And again, all of these, the crux of them is that they have important consequences for consumers. And the full list is available in our proposed draft of the regulations, which is also available on online. As an example. Okay. Perfect. Thank you. As an example of the use of ADMT for a significant decision, this would include things like a video screening technology, for example, that's used as part of a job interview.

So a business would be using that technology, for instance, to analyze a job applicant's body language, their facial expressions or their gestures to determine whether they would be a good employee and should be hired. If a business was using that technology to determine that type of hiring decision, that would be a use of ADMT for a significant decision about a consumer.

Turning now to the second use case, the use of

ADMT for extensive profiling. As you may recall, profiling generally refers to evaluating a consumer using automated processing. And when we talk about extensive profiling, we're generally talking about three types of profiling. So the first would be work or educational profiling. So this is profiling someone who's acting in their capacity as a job applicant, a student, an employee, or independent contractor, through systematic observation of their activities. So, for instance, using a productivity monitoring software to track how quickly workers are, for instance, packaging goods or completing projects that would be extensive profiling of someone.

Second, public profiling. This would be profiling a consumer through systematic observation of a publicly accessible place. So for example, using a facial recognition technology in a stadium or in a mall would be an example of public profiling.

And then lastly, profiling for behavioral advertising. That would be profiling a consumer to target ads to them. So all three of those are extensive profiling and the use of ADMT for each of those would be subject to the proposed requirements, which we will talk about.

Now turning to the last use case, these are the training uses of ADMT. That is when a business is using personal information to train ADMT that could be used for

significant decisions. So for instance, training an ADMT that would be used to make decisions about which consumers would be offered business loans to identify people.

So that would be training, for instance a facial recognition technology for physical or biological identification or profiling. We're going to talk a bit more about that term, but this would include, for instance, training a technology that analyzes people's facial expressions or their gestures to infer their emotional state.

And then lastly, to generate deep fakes. So this would be training an ADMT that could be used, for instance, to generate fake images of real people that would be presented as truthful or authentic. So, now that we've talked about those three uses of ADMT, I'm now going to turn it over to my colleague, Ms. Anderson, to talk about what the proposed requirements would be for those uses.

MS. ANDERSON: Thanks, Neelofer. Can you hear me?

UNKNOWN MALE: We do.

MS. ANDERSON: Great. Okay. So what would a business have to do if it actually used ADMT in one of those three ways? Specifically, the business would have to provide a pre-use notice to the consumers whose information it wants to process using the ADMT. It would have to give those 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.

And the consumers could exercise that right later if they chose to proceed with the business' use of the ADMT. We'll walk through each of the -- each of those in a bit more detail now. So starting with the pre-use notice. Before a business could use ADMT in any of those three ways that we just discussed, the business would have to provide the pre-use notice to the consumer so that the consumer could decide whether to opt-out or to proceed with the business' use of the ADMT and whether to access more information about the business' use.

The pre-use notice itself would have to include several pieces of information. First, why the business wants to use the ADMT to begin with. And the business would have to provide that specifically not using generic terms like, to improve our services.

Second, it would have to include information about how the ADMT would work. That includes information about the logic used in the ADMT, including the key parameters that are used to affect the output of the ADMT. It would include the intended output of the ADMT.

So oftentimes this would be something like a score that it may be creating about a consumer, or it could be

placing them into specific profiles or advertising segments. It would also have to include how the business plans to use that output, including any role of human involvement in the use of that output.

So for example, if the business were using an output score from a resume screening tool to determine who would be offered an interview, the business would need to disclose that that's how it plans to use the tool and the role of human reviewers in that process. The pre-use notice would also have to include a description of the consumer's right to opt-out of the use of ADMT and instructions about how the consumer can exercise that right.

Similarly, it would have to include information about their right to access information about how the business used the ADMT and how they could submit that request. Finally, the notice would have to include that the business is prohibited from retaliating against consumers for exercising those rights, any of their CCPA rights.

Next slide. Thanks. Okay. So what would a business have to do if a consumer then did opt-out of the business' use of the ADMT? If a consumer opted out of the pre-use notice stage before the business actually used the ADMT to process their information, the business would not be allowed to start processing their information in the first place.

If a consumer went ahead with the business' use of the ADMT and then decided to opt-out later, the business would have to immediately stop processing their personal information using that ADMT. And would also have to communicate that opt-out to anybody else that is involved in the process like it's vendors or service providers, that they also need to stop processing the consumer's personal information using that ADMT.

I will note that there are exceptions to when a business must provide an opt-out, and we'll talk about that next. One thing to note here as well though, is that there's no exception to providing an opt-out to the profiling for behavioral advertising or for the training uses of ADMT. A business would always have to provide the consumer with the ability to opt-out of those two uses of ADMT.

So for the exceptions, the first is an exception for security, fraud prevention and safety. This applies when a business wants to use ADMT for profiling in the workplace or educational settings or for public profiling. In these cases, a business would not be required to provide the ability to opt-out if it's using the ADMT only for security, fraud prevention or safety. To rely on the 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. This would apply when a business wants to use the ADMT to make a significant decision concerning a consumer. Such a 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 reviewer.

That -- to qualify for that exception, the business must generally provide the consumer with the method to appeal the decision to a human reviewer who's qualified to review the decision and has the authority to overturn it. 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 exceptions is the evaluation exception. This applies when a business is using ADMT for certain decisions such as admission, acceptance or hiring decisions. Allocation or assignment of work and compensation decisions or for worker educational profiling.

A business would not be required to provide an opt-out from the ADMT if the business has evaluated the ADMT to ensure that it works as intended for the business' proposed use and does not discriminate on the basis of protected classes. The business also would have to have implemented accuracy and non-discrimination safeguards.

Now, if a consumer proceeded with the business'

use of the ADMT, they can request more information about how the business used the ADMT with respect to them. If a consumer requests that access, then the business' response to the consumer would have to include several pieces of information. First, why the business used the ADMT. So again, 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 it were a score that was generated about consumers generally, the business would have to provide the consumer with their particular score. It would also have to include how the business used the output with respect to that consumer.

So for example, if the business were using the ADMT to make a significant decision concerning the consumer, the business would have to be providing what the role of the output. So the role of that score and the role of the human involvement in making the ultimate decision about the consumer. It would also have to include the logic of the ADMT, including the key parameters that affected the output and how they applied to the consumer.

So the specific pieces of information about the consumer that resulted in that score, that in turn resulted in the ultimate decision about them. The response to the access request would also again have to include information

about their other CCPA rights and that non-retaliation disclosure that businesses are not permitted to retaliate against consumers for exercising their rights.

I'll note here that a business that's using personal information to train ADMT, is not required to provide an access response to the consumer. In addition, a business that makes an adverse significant decision concerning a consumer using ADMT has additional notice requirements. Adverse significant decisions include things like being demoted or terminated from a job, being denied housing or essential goods or services, and other important consequences as Neelofer highlighted earlier.

So why is an additional notice necessary under these -- under these conditions? It's to ensure that a consumer knows when a business has made a significant adverse decision about them using ADMT. There may be a long time between when they have first received that pre-use notice and when the business makes an adverse significant decision. And consumers may have a preference not to exercise their right unless the business has in fact made an adverse significant decision about them. So the additional notice makes sure that the consumer can make an informed choice about whether to exercise their rights.

Lastly, if a business is using physical or biological identification or profiling for significant

decisions or for extensive profiling, it would have additional requirements. When we talk about this type of profiling, it generally refers to evaluating people using ADMT with information about their physical or biological characteristics.

Examples include things like facial recognition technology that analyzes your face and particular facial measurements to identify you. It would also include emotion assessment tools that evaluate your eye movements and other facial movements or gestures to analyze or infer your emotions or behavior.

A business that uses physical or biological identification or profiling for significant decisions or extensive profiling, must evaluate it first to ensure that it does work as intended for the business' proposed use and does not discriminate on the basis of protected classes. And the business must also implement accuracy and non-discrimination safeguards.

MS. SHAIKH: All right. So now we're going to turn to our second topic, which is risk assessments. So a risk assessment generally refers to identifying risks in this case to consumers privacy of a given activity and mitigating those risks. And the goal of a risk assessment here is to make sure that businesses don't do things with personal information when the risks to consumer's privacy outweigh

the benefits of that activity.

So who would need to conduct a risk assessment? Again, this would apply only to businesses under the CCPA. And assuming you are a business under the CCPA, you would need to conduct a risk assessment before first selling or sharing personal information.

Second, processing sensitive personal information. When we say sensitive personal information, this includes things like social security numbers, certain financial information, your precise geolocation information, your health information, as well as -- it would also include children's personal information. So this would be the personal information of consumers that a business knows is -- are less than 16 years of age. It would also require risk assessment before using automated decision making technology for a significant decision.

And as a reminder, those are those decisions that have important consequences for consumers such as the decision to hire or fire them, or for extensive profiling, that's the worker educational profiling, public profiling or profiling for behavioral advertising. The use of ADMT for either of those significant decisions or extensive profiling would also require a risk assessment.

Lastly, training, Automated Decision-making Technology or Artificial Intelligence in certain ways would

also require a risk assessment. This would be training those technologies that could be used for a significant decision about someone to establish individual identity for physical or biological identification or profiling to generate deepfakes or to operate generative models. The training of ADMT or AI for any of those uses would also require a risk assessment.

For each of those four uses, a business would conduct a risk assessment. So what would a risk assessment generally involve? At a high level, it would have to include the following. So first, why the business actually needs to do the activity. So what's the purpose of it?

Second, the types of personal information that the business would need to collect, use, disclose, retain or otherwise process to do the activity and whether it involved sensitive personal information. Third, how the business would actually do the activity.

So this would include important operational elements. Things like how many consumers personal information would the business need to collect, what disclosures the business has made to those consumers about the use of their personal information. Who else might be involved in the activity such as vendors, and which technology the business plans to use to do the activity. These are all important operational elements that directly

affect the risk of a given activity. So it would be important to identify them.

Next, a business would also need to identify, four uses of ADMT for significant decisions or extensive profiling, certain additional information about how that technology works. So this would include for instance, the logic of that system, what the output is, and how a business actually plans to use that output for a significant decision or extensive profiling.

Next, and this is perhaps the most important part of the risk assessment, which are the benefits and consequences for consumers. A business as part of its risk assessment would identify the benefits of that activity as well as the consequences. So the negative impacts to consumers privacy that could result from that activity and any relevant protections or safeguards that the business plans to or has already put in place.

Lastly, the business would identify whether it actually plans to initiate that activity. So what was the conclusion of the risk assessment and details about who contributed to, reviewed and approved the risk assessment, and when those reviews and approvals happened.

An important note here, again, with the goal of a risk assessment being to stop activities where the risk outweigh the benefits. A business would in fact be

prohibited from starting any of those four activities we talked about if the risks to consumers privacy outweighed the benefits of that activity.

So now that we've talked about what would be in a risk assessment, the next question would be, when would you actually have to conduct or update one? So importantly, a business would need to conduct a risk assessment before starting any of those four activities.

And this makes sense because if the whole point is to make sure to identify risks to consumers' privacy and mitigate those risks, you need to do so before you start that activity rather than in the midst of it. In addition, a business would need to review those risk assessments every three years to ensure they remain accurate and update them as needed.

And lastly, a business would need to immediately update its risk assessment whenever there's an important change to that activity. So for example, if a business realized that it needs to collect more sensitive personal information about someone, that would be an important change that would require immediately updating the risk assessment to identify any additional risks to consumers' privacy that could result from that change, as well as identify any important safeguards to be implemented.

All right. Now that we've covered what a risk

assessment would include and when a business would conduct one, we're now going to talk about what a business would actually have to submit to our Agency and when. One of the requirements of the CCPA would be that a business would submit its risk assessments to the Agency on a regular basis.

So what would need to actually get submitted? So first, a business would need to submit a certification of compliance. This would be a certification by the highest ranking executive at the business in charge of risk assessment compliance, that the business conducted a risk assessment before starting any of those four activities we talked about. That would be submitted to the Agency with abridged forms of every risk assessment that the business conducted during that time.

And when we talk about abridged form, that's essentially a risk assessment in short form, and that would identify four things. So first, what was the activity that actually triggered the risk assessment? So for instance, was the business selling or sharing personal information? If so, it would identify that as the relevant activity.

Second, what was the purpose of that activity? And then third, what categories of personal information did the business need to collect, use, disclose, retain, or otherwise process for that activity. Lastly, and

importantly, the business would also identify what protections it put in place for that activity. So these four things would be part of the abridged risk assessment and would be submitted to the Agency.

So when a business would submit them, there's two things to keep in mind here. So first, a business would have 24 months to submit its first certification and the first batch of abridged risk assessments to the Agency after the effective date of the regulations. So 24 months from the effective date. After that, it would be submitted every calendar year after that. So ongoing certifications as well as any new or updated abridged risk assessments, those would be submitted every year after the first submission.

Lastly, for unabridged risk assessments. So that would be the full risk assessment that contains all of the items I discussed earlier. Those would need to be submitted to either the Agency or the California Attorney General if they were requested. So upon request, a business would have 10 business days to submit its unabridged risk assessments to either the Agency or the California Attorney General.

Now, one final note that I'll make about risk assessments, is that we are aware that other states and other countries have similar requirements for businesses or in other cases these are often called controllers. And really there's no requirement to duplicate your efforts. If

a business is conducting a risk assessment for the same activity to comply with other states or other countries as well as the CCPA, it would not be required to redo it for the CCPA.

However, it would need to add to it as needed to address any CCPA requirements that were not addressed under other states or other countries. All right. I'm now going to hand it off to Ms. Anderson to talk you all through a couple illustrative examples that kind of show how these things all work together.

MS. ANDERSON: Thanks, Neelofer. So, now that we've provided a bit of an overview of the Risk assessment and ADMT requirements, we'll talk through two examples of business activities and what the business would have to do under the proposed risk assessment and ADMT requirements. These examples don't cover all potentially applicable laws or enforcement circumstances. So, we thought that the examples may be helpful for businesses seeking to understand how the draft regulations would apply under a few given circumstances.

So the first example is a retailer that wants to use facial recognition technology in its stores to identify shoplifters. What would the retailer be required to do under the proposed regulations? First, the retailer would have to conduct a risk assessment. It would also have to

evaluate the facial recognition technology to ensure that it works as intended for the retailer's proposed use and does not discriminate, and it would have to implement accuracy and non-discrimination protections.

So, for example, certain facial recognition technology may be known to be less effective or less accurate with respect to certain demographic groups depending upon the conditions like lighting conditions or how the hardware is set up. So the business' accuracy and non-discrimination protections could include things like ensuring that the lighting is appropriate and that there is appropriate signage in the particular locations where it is deployed.

The business also would have to provide a pre-use notice to consumers, and it would also have to provide consumers with the ability to access more information about the use of the ADMT. The retailer would not have to offer an opt-out from its use of the ADMT as long as its use is only for the fraud prevention. Fraud prevention in this instance includes resisting, malicious, deceptive, fraudulent or illegal actions that are directed at business and to prosecute those responsible for those actions.

Our second example is a business whose HR team 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, which the manager will then use to determine which of them will be promoted.

So what would the business be required to do under the proposed regulations? The business would not have to conduct a risk assessment and would not be subject to the ADMT requirements. That's because the business would be using the spreadsheet merely to organize the human decision makers evaluations. So this wouldn't be ADMT in the first instance. Recall that ADMT requires businesses that use the technology to -- using the technology it would have to be to replace or substantially facilitate human decision making.

We will now pivot over to the Cybersecurity Audit requirements. Our proposed cybersecurity audit requirements are designed to ensure that businesses that meet certain thresholds independently and thoroughly assess how they protect consumer's personal information.

Taken together the proposed requirements will help businesses to identify and remediate problems in their cybersecurity programs, resulting in further protections for consumers personal information. So today we will cover who would need to complete a cybersecurity audit and then what a business and its auditor would have to do to complete the audit. That second portion will include how the business would complete the cybersecurity audit, who the auditor

could be and what they would have to do, what the audit itself would include, and when the business would have to complete a cybersecurity audit.

So in terms of who would need to complete an audit, assuming you are business under the CCPA and that terms defined in the statute, and Neelofer provided some guidelines for that earlier, you would have to meet one or both of these two thresholds on the slide to be subject to the cybersecurity audit requirements, meaning that you would have to conduct an annual cybersecurity audit.

The first threshold is a business that made more than half of its annual revenue from selling or sharing consumer's personal information in the preceeding year. The second would be a business that made over $28 million in annual gross revenue in the preceeding year. And processed meaning either collect, use, retain, disclose or otherwise process the personal information of 250,000 or more consumers or households or process the sensitive personal information of 50,000 or more consumers in the preceeding calendar year. And again, sensitive personal information will also include the personal information of consumers that the business knows were under 16 years of age.

So what would the actual -- what would a business actually have to do to complete their cybersecurity audit? There are four main things that it would have to do. First,

it would need to select an auditor and we will cover the requirements that auditors would have to meet on the next slide.

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

Third, the business would have to report the audit results to the most senior individuals in the business responsible for the cybersecurity program. There would be guardrails in place to make sure that the business did not improperly influence the auditor as they complete their audit. But at the end of the day, it's the people who are responsible for cybersecurity, who most need to know what the audit results were so that they can understand how they're doing and where to focus their attention to better protect consumer's personal information.

Forth and finally, the business would have to submit a certification of completion to the Agency through the Agency's website. The certification, much like with risk assessments, would be signed by the most senior individual in the business who's responsible for cybersecurity audit compliance. It would certify that the

business had completed the audit as set forth in the draft regulations and also that the signer had reviewed and understands the findings of the audit.

So who could the auditor be? As we just discussed, the business would have to select the auditor, but the auditor can't be just anyone. They would have to be qualified, unbiased and independent, and they would have to be using professional auditing standards and procedures. Those that are generally accepted in the profession of auditing. The auditor could be somebody who's working in the business or be an external auditor outside the business. So if a business already employs someone who meets the requirements on the slide, that person could become their cybersecurity auditor.

Now that we have covered who the auditor could be, we will get into the three main things that an auditor would actually have to do to complete the audit. First, the auditor would determine which of the businesses systems would need to be audited and how to assess them. They would likely do that based upon their expertise and the information provided by the business. That information would include things like where and how the business collects processes and stores consumer's personal information.

Second, the auditor would independently review

documents, conduct tests, and interview the appropriate people to support the assessment of the business' cybersecurity program. The draft regulations list parts of the business' cybersecurity program that the auditor would have to assess document, and summarize, and we will cover some of those as well as what the audit would have to include on the next slide. Third, the auditor would have to certify that they completed an independent and unbiased audit.

In terms of what the actual cybersecurity audit would include. The next two slides talk more about all of that, and we break down what an audit would have to include generally into eight key pieces. First, the audit would have to include a description of the systems audited. Second, it would have to include the information the auditor used to make their decisions and why that supported their findings. This would include why they scoped the audit the way that they did.

So, for example, why some systems were in scope, but others were out of scope, why they assessed the systems and components of the systems the way that they did, what evidence they examined to make their decisions and assessments. So for example, which documents they reviewed, what kind of sampling and testing they performed, the percentage of systems tested in the interviews that they

conducted. And they would have to explain why all of this was appropriate and sufficient to justify their findings.

Third, the audit would have to include the auditor's assessment of how the business protects consumer's personal information through its cybersecurity program. That would include the written documentation of the cybersecurity program, including the cybersecurity policies and procedures. And it also includes the common ways that businesses protect personal information such as authentication, how it ensures that its employees and its customers are who they claim to be when they are accessing personal information. How the business uses encryption to protect consumer's personal information and how, for example, it's prepared to handle cybersecurity incidents.

Fourth, the audit would have to describe how the business follows its own policies and procedures. Written policies and procedures are not worth very much if people are not aware of them or are not following them. So the audit would be looking into this as well.

Fifth, the audit would have to describe the gaps and weaknesses in the program and how the business plans to address them, including the resources it's allocated to resolve those issues. And the timeline for resolutions. This is part of how the audit assesses the effectiveness of the program.

Sixth, the audit would have to include a description or sample copy of data breach notifications that were sent to consumers or agencies. You have all probably received several of these as well as information related to those breaches and the fixes. So for example, the gaps or weaknesses that permitted the breaches in the first instance and when and how they have been fixed.

Seventh, 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 the cybersecurity program.

Finally, the audit would have to include the certifications both from the auditor and the business that the audit was independent and unbiased and not subject to any influence or attempted influence by the business.

Now that you have a sense of who would be responsible for what and what would have to be included in the audit, let's talk about when all of this would need to be done. Much like with risk assessments, a business would have 24 months from the effective date of the regulations to complete its first cybersecurity audit. Thereafter, it would have to complete the cybersecurity audit and submit its certification annually. So every year thereafter.

There also cannot be a gap in the months that are covered by successive audits. One final point we will make

regarding cybersecurity audits is that there is not a requirement for a business to complete a duplicate audit or a duplicative work. If a business is completed a cybersecurity audit assessment or evaluation for some other purpose, and what it's done already meets the requirements in our draft regulations, then the business would not be required to redo that same audit. Instead, it would have to add to it as needed.

So if it did not meet all the requirements, the business would have to supplement it with any additional information necessary to meet all the requirements. And next, I will pass to Phil for how to participate in the formal rulemaking process.

MR. LAIRD: Well, thank you all. We know we just hit you with a lot. But that is a pretty comprehensive overview of what we're proposing to do with these regulations. So now I'm just going to take a moment to talk a little bit about where you can engage beyond today. And so first and foremost, you will have an opportunity today to give public comment and we are looking forward to that.

But in terms of where we are in the rulemaking process under state laws as of today we are in step one, which is the preliminary rulemaking stage. Where we are still refining draft regulatory text based on our Board's feedback and drafting the necessary documentation that would

allow us to start formal rulemaking.

But I want be very clear, and I know our chair mentioned this earlier before step two, formal rulemaking can begin. The Board will receive and review that package of documents review and has to make another vote to actually move these draft regulations into formal rulemaking. We are not to that stage yet.

But step two, once that vote occurs and that documentation is finalized, the Agency would then publish the notice to proposed rulemaking, which would kick off what is a standard 45-day public comment period. During that time, the Agency can receive written comments as well as we well host a public hearing to receive oral comments, much like we will here today.

And after the public has provided comments, the Agency considers the feedback and responds to them. The Board then will consider to the extent which it wants to make modifications to these proposals based on that feedback. So you can see this process is thoughtful. It gives an opportunity to review that feedback and then another opportunity for our Board to consider if changes need to be made because of things raised by you all and by the public.

The Agency once it reviews in response to all public comments for a final time, it would finalize the

rulemaking package and send it to review within office in the state called the Office of Administrative Law. The Office of Administrative Law, which is unconnected to our Agency, and it's an objective third party reviewer would review the rulemaking package for compliance with our procedures that we have to follow under state -- under the state law. And they would have 30 working days to do that.

If OAL, Office of Administrative Law approves that regulatory text in the package, then it would be filed with the Secretary of State and actually become regulations that are enforceable.

So in terms of participating in public rule make -- or public rulemaking generally, but specifically with our Agency, we have a few tips to share with you. Again, first off, you're off to a great start. You are already here today to make some public comment. We are very appreciative of that. But when we are in formal rulemaking. First of all, we would say please do subscribe to our email list to receive updates on the rulemaking process. Specifically, you will get a notice of this email when we have entered that 45-day public comment period, so you are well aware of when you can submit those formal comments.

Secondly, you can attend our Board meetings and public hearings. The agenda for Board meetings are always posted on our website at least 10 days in advance. You can

also watch recordings of past meetings and actually every agenda item the Board hears, there is an opportunity for public comment then as well. So again, ample opportunities to provide feedback.

And lastly, you can submit your public comments, as I have mentioned a lot during the formal rulemaking period, that 45-day public comment period. Or if we do additional comment periods because of changes to the text, you will have additional opportunities then as well.

So with that said last thing I will just note is a lot of this information is available on our website, including the handouts at the back of the room. So I will be remiss to not promote our website a little bit for the Agency, it is CPPA dot ca dot gov. However, we also have a more consumer focused and business focused website available. That is privacy dot ca dot gov and we will encourage you all to look at the resources and information there.

Again, we understand you are probably ingesting a lot today. You can take much more time to review those materials and concepts we have discussed on those websites. So thank you. I will now turn it over to Megan to introduce our public comment portion of our event today.

MS. WHITE: Wonderful. Thank you so much. Okay. So now we're going to move into the public comment period.

We'd appreciate it if you came up to this podium to make public comment if you are able to physically do so, just so we can make sure that we capture your words. If that's not possible for you are welcome to get public comment from your seat.

Since we have a small group today, I don't think that there's any need to form a queue. You are welcome to just come up here. You have five minutes for public comment. I am going be sitting right about in the middle of the room. I will be timing you when you have one minute left. I will give you the one minute signal and then you will hear my alarm go off when we are at the five minutes. So it's now open to you all. Feel free to come up here if you'd like to make a comment.

MR. VASQUEZ: Be reading this all from my phone because this is not a normal thing for me. But hello, I am Brian Vasquez. I am a local illustrator, born and raised here in Fresno. I am also currently a Fresno resident. I am an artist who has to use drawing programs like Adobe Photoshop, which has recently gone on to incorporate AI in their drawing programs. Knowing that some of the data use to train Adobe's AI model for their AI add-on Firefly gave me no choice but to use other programs that I might not necessarily be used to.

If they have to use it, artists are trying to do

anything to keep their art from being stolen by using apps like Nightshade and Glaze, which I use which can affect the quality of the appearance of their work, which can be critical in terms of getting future work due to the nature of the art industry's visual format. I have to post it on my social media. It has to look great. It doesn't look so great when I have to use those apps. Just to you know protect my work. Our work must always look its best aesthetically.

Concerning drawing programs like Adobe Photoshop's, ill-gotten data. This is an ethical issue I take to heart, which is using drawing programs that will use my data information to train more AI models without the ability to opt out. Also, these AI models will use artist names and their art style to generate art immediately. There are indeed forgeries of that artist's work and art style all generated off of their name used as a simple word prompt. An artist's particular style or trade dress are everything in this industry.

An artist's trade dress is the very reason why they are sought after for some jobs. It is sometimes the only reason they are a desirable artist. Think of the style of Pablo Picasso or art in the style of Da Vinci. Well, they are gone. But these days, artists that are alive are having their data stolen while they are alive today.

For an individual artist, there are very few alternatives to use these drawing programs, which are taking my personal information like my art style. This is something that I have cultivated through years of study with no kind of regulation or filter blocking my name from being used for a word prompt or training the life of an artist is in danger even of you know having a future, especially competing in an unfair competition with AI which can prompt hundreds of images in minutes.

I will like to make it very clear. An artist's art style or trade dress is an encapsulation of everything they have learned and haven't learned. What is happening now within a -- with AI is our personal styles are now being stolen from our -- from us per our data information that is also being used as a prompt by prompt pirates that we artists are now having to compete with in order to survive. This nightmare scenario is only happening because there is no regulation. There must be reasonable regulation that expands the definition of deepfakes to include deepfake forgeries that copy an artist style or trade dress.

There should also be a very clear filter or ban on artist names being used as prompts for AI . Artists are seeing real world ramifications of AI competition, which is based of ill-gotten data of our own. The methods for acquiring this data must also be addressed in its

regulation. The art industry is a competitive when AI brings that competition to a breaking point, all born of stolen data. And that is why there needs to be real regulation now. Thank you.

MS. WHITE: Thank you.

MR. SINGLETON: Good afternoon, chair, staff. My name is Robert Singleton. I am the Director of Policy and Public Affairs for California and the West US region for Chamber of Progress. We are a tech industry association supporting public policies to build a more inclusive country in which all people benefit from technological leaps. I have some prepared remarks about just the general approach and some concerns we have with the ADMT regulations.

But going off the cuff here a little bit and using some of the examples that we saw by staff, I am really concerned about how this affects consumers and how they are treated in aggregate in particular as it comes to our businesses going to be allowed to incentivize either opting out or non-opting out. So what I mean by this is if I don't -- if I don't opt in to having my personal information used to hopefully improve my user experience using an app or something like that. And let's say the business provides incentives for opting in, for using my data, so specialized offers, discounts, things like that nature.

Is the fact that I -- who opted out did not

receive access to these benefits or offers or other potential things, is that inherently retaliatory towards me as the one opting out? It's an interesting question because if the answer is yes, then are we explicitly not allowing for incentives for participating in trading information and data essentially for discounts preferred customers -- You know, some real use cases here especially if you know -- if you fly a lot like I do every week having access to being frequent flyer miles and other programs are real boon.

But if we are saying that those can be allowed and if I do opt out and that's non-retaliatory, does that mean that we're inherently codifying a preferred track for consumers? So that there's going to be a group of consumers who unilaterally opt into things and then massively benefit across every single business or application or marketplace they participate in. By being a preferred consumer, the ones willing to share their data. Whereas those who are not willing to share their data for very legitimate privacy concerns, intellectual property, artist style, things like that are now relegated to being not preferred consumers across many different apps, marketplaces and in settings.

So it's a big concern that I have just personally and looking at the process and I think it's not really addressed in the regulations they've seen thus far and so really answering that question of what is retaliatory in

terms of businesses being able to offer things that I think would be beneficial to consumers in their experience. I also worry generally about training data and AI and what's already been used to train existing models. What are we going back to retroactive data privacy in terms of everything that I've ever put into a Google search engine that could be attributed to me.

If we're looking at app stores in particular, I don't know if you guys looked at it but Open AI made a big product announcement this week as did Google with their entire Gemini 1.5. I was at the Google IO conference yesterday, they're now designing every single Google device, every single Google application, all their sub applications, all the developers are all going to be based upon Gemini, their core AI engine, their core frontier model built into everything they do. So to what extent does Google have an onus to provide opt-out their app Developers have an onus to do this different device, people who publish things, people who sell right to repair kits who are utilizing personal information.

The -- how this manifests a digital marketplace could be potentially very problematic when we're going rapidly towards a place where AI is going to be on every single device and a part of every single consequential decision that we make in the economy just as consumers

that's where we're headed. And so this -- what is could be quite a lot of layers of compliance for a business. Maybe it's easier for Google to do but for two people working on an application in the garage trying to make it big and a startup having to have what essentially could be a compliance attorney and an auditor and having to submit all these things could be a pretty impactful to their business and their ability to survive and thrive.

As an example, I'll say I used to work for a carbon accounting startup where we helped businesses and cities and governments reduce their carbon footprint by taking in a lot of data, making recommendations about building footprint, about employee travel habits, about parking I mean all these things. And if we didn't have access or if someone could opt out preferably or if we were doing a business park and there was individual vendors there that each had different employees or different consumer markets not having access to that data would certainly not be able for us to provide our core business offering. But at the same time where's the balance between the individual folks who are -- would ultimately benefit from reducing carbon footprint there. An example being, let's say someone ops out to be considered --

MS. WHITE: I'm sorry, that's five minutes. But we -- certainly you're welcome to come back up after we allow

everybody else.

MR. JEW: For having these traveling listening tours, Government hearing concerns of its constituents is the cornerstone of our democracy and I thank you all for doing this. My name is Benton Jew and I'm an illustrator in the film industry. I've worked professionally for over 36 years. My twin brother and I learned how to draw small children, learning to develop the skills that are necessary to draw and create beautiful images and tell stories. It takes a lifetime of work, study, trial and error practice to do what we illustrated do well. And proud to say I've made a decent middle class living doing it.

The past couple of years, generative AI has exploded upon the public seemingly out of nowhere using billions of images scraped from the internet without the knowledge and consent of the images originators. This was originally done under the guise of research and development and was not supposed to be used for commercial purposes. Thousands of illustrators have found their work used to train AI data sets. Even all of my very own private personal Christmas cards have made their way into the data sets without my prior knowledge or consent. I can't even advertise my own work online without fear it will be acquired for commercial purpose.

I have almost no control how my password can be

used anymore when used to be able to buy Photoshop and you could work offline and nobody could access your work but you. Now with the new subscription models with the cloud-based storage in order to use Photoshop, there are no -- you are no longer able to keep your work solely offline leaving yourself vulnerable to data scraping. Production llustrators are often required by our employers to use certain software in their pipelines and those software's are actively stealing our data, while we use the programs for work.

We are often forced to interface with a computer program that is literally stealing from us in the present to replace us and devalue us in the future. If all data is free for the taking by large companies, artists could lose control of the thing that makes them unique and saleable. If everyone can be Van Gogh, there is no Van Gogh. If everyone can be Gerald Schultz (ph), there is no Gerald Schultz. Some artists make their living from commissions.

One artist that comes to mind whose livelihood has been entirely destroyed is an artist named Greg Rutkowski. His name has been used as a prompt in these AI programs more than 400,000 times. His name was used as part of a pull down menu that listed 4,700 artists who neither knew of or gave permission to be on that list. Deepfake forgeries of this work now run rampant across the internet. So now not

only is his ability to earn a living made impossible.

Fans and consumers of his work are being bamboozled by these fakes. Prompters can make their own Greg Rutkowski pieces to profit from. There are now so many fake Greg Rutkowski's that the real Greg Rutkowski's life has been ruined because people can't tell the reals from the fakes. His livelihood is stolen by an algorithm that facilitates forgery and theft.

An artist's style and trade dress are part of their marketability and more importantly their identity like a face or fingerprint or even a written signature by an artist on their network, on their -- by an artist on their artwork. An artist's style is unique. An artist's art style is as much a commodity to some artists as a face is to an actor.

AI data scraping is a way of stealing for you while you're creating new work leaving you no agency over the work you do or might develop for the future. Anyone can scribble a picture. Illustrators however, trained for years to make their scribbles have value. We add value to blank pages and feed our families with that value. Now that value is being stolen from us by our own tools. As easily as AI came to us, other tech that does not respect the privacy of citizens will pop up without guidelines in place more tech will pop up that violates people's right to privacy and in

the state with Silicon Valley an out of prevention is worth a pound of care. Thank you.

MS. WHITE: Thank you.

MR. LAIRD: To the gentleman that had been speaking earlier. If you want to continue your comment, you're welcome to.

MS. WHITE: I'll just start the timer for another five.

MR. LAIRD: Okay, great.

MR. SINGLETON: I'll read my prepared remarks just to -- and then I have some additional thoughts on AI and training data in particular so. So I'm here today to urge you to revise your approach and set aside your well-intentioned but ultimately problematic proposal to regulate automated decision making tools in lieu of the ongoing legislation and executive action relating to artificial intelligence which the rulemaking process stamp to potentially undermine the proposal. Rules impact assessment and safeguard requirements are excessive and potentially harm competition.

They expose business strategy and stifle competition by manning the businesses disclosed the details of their making decision tools to the public, so for instance an app developer,.any such disclosure of sensitive business practices must serve a compelling government

interest and be narrowly tailored. The draft rules come up a little bit short on both. This is doubly pragmatic because automated decision tools are essential for online platforms enhancing user experience through recommendations on products and services and fostering innovation where redacting trade secrets may offer some protection.

The proposed rules or -- excuse me, regulations extensive requirements risk handling proprietary strategies to competitors giving them valuable insights that would undermine competition and ultimately harm consumers. The CPPA's approach creates confusion over who is charged with protecting some Californians, again in the instance of online marketplaces and understanding the onus of liability and disclosure requirements in between platforms and the marketplaces and the folks who curate those marketplaces.

Remaining the proposed provisions are quite similar to policy being considered in the state legislature presently, so if the CCPA or CPPA and the state legislature are both act will create sometimes redundant or concerningly overlapping policies leaving developers unclear as to who is regulating them and the public unclear on who is protecting them. It's also possible that any rules propagated by the CPPA would quickly be obviated by the legislature. The CPPA should pause at least until the people's elected representatives have had a chance to opine through this at

the end of this session's term.

In September 20th, 2023, Governor Newsom published his executive order which called for whole of government approach to AI policy. Indeed, the executive order took pains to balance innovation and consumer protection as discussed below. In contrast the CPPA's Automated Decision-making Tools proceeding stand to duplicate much of the work of this administration once again creating confusion for developers and the public alike. Policy can protect consumers without squandering California's tech leadership. We commend the CCPA or CPPA for considering the potential harm for automated decision making.

The current proposal adds substantial regulatory and compliance burdens to California startups without obviously advancing consumer privacy. For example, the proposal mandates software developers create a mechanism to offer consumers the ability to opt out of hotel or flight upgrades preferred track for customers and few, if any, customers would ever want that. Nevertheless, the rules as drafted would obligate every small hotelier to develop that functionality.

A better approach would be to work with stakeholders to identify areas where drafting can be improved and tailor the rules narrowly to advance consumer protections in those key sectors. On the notion of AI

training data, since I still have some time, this is a really hard one in terms of being able to tie inputs of training data towards outputs not necessarily with Gen AI but with any kind of automated decision tool.

Many of the most sophisticated frontier models are ingesting billions upon billions of data input streams and optimizing those often times without any human supervision knowledge of the inner workings in every single billionth iteration of which data point is being used and correlated to what, and so it's oftentimes really hard to take inputs and clearly understand how they were articulated, processed and then utilized to render a series of given inputs and it can be really hard and technically difficult, so not only just legally, but technically difficult to try and figure that out, and for a brand new agency to try and bite off that apple, what is largely going to be somewhat of a transcendental economic technology that's going to be a part of all of our -- every part of our lives, every device that we have here it's going to be -- it's a difficult regulatory task, especially to try and lower away the folks who actually have the technical capacity to be able to weigh in these in a sophisticated and competent manner.

Your average AI developer right now is baking at least $350,000 a year in base salary probably upwards towards a million if they're really good. So being able to

lure that talent from the private sector to be able to trace back how the inputs and outputs align and where the disclosure and the onus on which part of that chain, whether it's a frontier model or maybe a kernel you downloaded and personalize or fine tuned and trained as a developer that you apply to a specific use case. And then my biggest worry is that this may perpetuate biases because you have a large group of people who do opt out of being part of the training data and then the outputs are inherently biased towards those who opted in versus those opting out creating what could be codified bias in again people's economic and consumer experience.

MS. WHITE: Thank you.