AMENDED TRANSCRIPTION OF RECORDED STAKEHOLDERS SESSION OF CALIFORNIA PRIVACY PROTECTION AGENCY

MAY 4, 2022

VIA TELECONFERENCE

Present: ASHKAN SOLTANI, Executive Director
BRIAN SOUBLET, Interim General Counsel
JENNIFER URBAN, Chairperson
TRINI HURTADO, Conference Services Coordinator

Transcribed by: Alaina L. Russell,
eScribers, LLC
Phoenix, Arizona

--o0o--

AMENDED TRANSCRIBED RECORDED PUBLIC MEETING

OF CALIFORNIA PRIVACY PROTECTION AGENCY

May 4, 2022

MR. SOLTANI: We can get started. Good morning, everyone. Welcome to day one of the California Privacy Protection Agency's May 22nd -- 2022 Pre-Rulemaking Stakeholder Sessions. My name is Ashkan Soltani and I'm the executive director for the agency. Please note that this event is being recorded. We are delighted to have many -- so many stakeholders sign up. And today, our board chairperson, Jennifer Urban, will provide a brief welcome, then I will introduce (indiscernible) and we'll go over logistics and then we'll go straight into our first topic.

Chairperson Urban?

MS. URBAN: Thank you Executive Director Soltani.

Good morning, everyone. My name is Jennifer Urban. I am the chairperson of the board for the agency. I'd like to thank our executive director and all of the staff who have been working on this for inviting me today to go over our pre-rulemaking activities and to invite your participation over the next few days.

These stakeholder sessions are the third of the agencies pre-rulemaking activities. The first activity was an invitation for comment that invited written

comments from stakeholders. The second activity was a set of pre-rulemaking informational sessions held in April. The informational sessions provided background information on various topics potentially relevant to our rulemaking.

The speakers for the informational sessions were academics who study relevant topics as well as officials from the California Office of the Attorney General, the California Privacy Protection Agency, and the European Data Protection Board, and I expect and hope some of you joined us for those.

The written comments from the invitation for comments as well as the recordings and transcripts at the informational sessions are all available on the CPPA website if you're interested in reviewing them.

This event, the stakeholder sessions event, is the third pre-rulemaking activity. While subcommittees of the board provided input to the previous activities, the process has now been turned over to our staff who have organized these stakeholder sessions to further inform the rulemaking process. I was delighted to hear of the very strong interest in the sessions and the large number of stakeholders who signed up for stakeholder speaking slots for this event.

I believe Executive Director Soltani will say more

about how the event will proceed, but I would like to encourage anyone who's interested in speaking that has not signed up for a formal slot, to consider speaking during the time each day for general public comment. There's no need to sign up for that, just like there's no need to sign up to listen. You can just click on the link, join the Zoom, and then if you'd like to speak during general public comment, just raise your hand during that part of the program. I know we're eager to hear from all of you.

The agency and the board are in listening mode. We are learning as much as we can. And as I mentioned, the agency staff are organizing and moderating this event. Board members, including me, will be in the audience with you.

I would like to thank Executive Director Soltani and all the agency staff for putting together such a robust program and providing this opportunity to hear from stakeholders. I would also especially like to thank everyone who participates over the next three days. We are eager to hear about your experiences and to receive your input. I'm really looking forward to this. Thank you.

MR. SOLTANI: Thank you, Chairperson Urban. Before we get started with the substance of the day, I

wanted to take a moment to thank everyone who has signed up or plans to comment during the public comment period. There are so many knowledgeable stakeholders (indiscernible) based on their specific experiences and expertise. For example, an individual business that has experienced implementing the CCPA's statutory language and regulations, an individual consumer that has experience trying to understand and exercise their rights and the expertise of their own viewpoint about what's important to them. Thank you all for joining.

I also want to thank all the staff working to make these meetings possible. I would like to thank the team from the California Privacy Protection Agency and the Office of Attorney General for supporting us today. Mr. Brian Soublet, who is hosting, and Ms. Trini Hurtado who is acting as moderator and has organized the meeting infrastructure, and Ms. Stacy Heinsen (phonetic) for organizing administrative staffing and resources.

I'd also like to thank the team at the Department of Consumer Affairs for managing our communications list on the website. I'd also like to generally thank the staff at the Business Consumer Services and Housing Agency, the Department of General Services, the Office of Attorney General, and other agencies who continue to help us behind the scenes.

And with that, I'd like to hand it over to our master of ceremonies, Mr. Brian Soublet, to go over logistics for the event. Mr. Soublet?

MR. SOUBLET: Okay, there's our first bug. Thank you, Executive Director Soltani.

Good morning and welcome to the California Privacy Protection Agency's May 2022 pre-rulemaking stakeholder session. I would like to remind everyone that this session is being recorded. I have some logistical announcements and will go over the plan for each session.

First, let me sketch the format of these stakeholder sessions so everyone has a sense of how things will proceed. As you can see from the program and schedule, which you can find on the meeting and events page of our website, we are holding a series of stakeholder sessions this week, May 4th, May 5th, and 6th. During the sessions, we will be hearing from stakeholders on a series of topics that are potentially relevant to the upcoming rulemaking.

Those who signed up to speak in advance were generally given a speaking slot for their first choice topic and will be limited to seven minutes. We will proceed through the program according to the schedule provided on the website. Please note that all the times are approximate and topics may start earlier than

estimated.

You are welcome to come and go from the Zoom conference as you'd like, but if you have an assigned topic, we recommend that you make sure you are signed in before your topic session begins. Even if you did not sign up in advance, you will have an opportunity to speak during the time set aside for general public comment at the end of each day. Please take a moment to review the schedule to see when public comment is expected to occur, and again, please note that the times are approximate. Each speaker making general public comments will be limited to three minutes. Please note that we are strictly keeping time for all the speakers in order to accommodate as many stakeholders as possible.

We look forward to hearing from everyone, and it is important to note that stakeholder's views should not be taken as the views of the agency or the agency's board. They are the presenter's views only.

Speakers that are scheduled for the automated decision-making session should be signed in to the public Zoom link using the name or the pseudonym and email they provided when they signed up to request their speaking slot. If you are participating by phone, you will have already provided the phone number that you are calling from so that we may call on you during your pre-appointed

speaking slot. You should note that your name and phone number may be visible to the public during a live session and the subsequent recording.

Speakers will be called in alphabetical order by the last name during this window and we will not be able to wait if you miss your slot. When it is your turn, our moderator will call your name and invite you to speak. If you hear your name, please raise your hand when your name is called using the raise your hand function, which can be found in the reaction feature on the bottom of your Zoom screen. Our moderator will then invite you to unmute yourself, and then you will have seven minutes to provide your comments. In order to accommodate everyone, we will be strictly keeping time, and speaking for shorter length of time is just fine. When your comment is completed, the moderator will mute you.

Please plan to focus your remarks on your main topic, however, if you'd like to say something about other topics of interest at the end of your remarks, you are welcome to do so. You are also welcome to raise your hand during the portion at the end of each day set aside for general public comment.

Finally, you may also send us your comments via physical mail or email to regulations@cppa.ca.gov by Friday, May 6th at 6 p.m. Note, California law requires

that the CPPA refrain from using its prestige to influence or endorse or recommend any specific product or service. Consequently, during your presentation, we ask that you also refrain from recommending or endorsing any specific product or service.

I now ask that the stakeholders who have been assigned to the automated decision-making topic be ready to present. Please use the raise your hand function in Zoom when your name is called so that our moderator can easily see you. As noted, the moderator will call you in alphabetical order by last name. We will now move to hear comments on the topic of automated decision making.

Ms. Hurtado, could you please call the first speaker?

MS. HURTADO: Hi. My name is Trini and I'll be your comment moderator for today. I'll be calling names in alphabetical order according to last name. If you're scheduled to speak in the session, you should have your hands raised already. Please do not raise your hands unless you've been confirmed. There will be a time during the public comment period at the end of each day for those wanting to make public comment.

When you have been called on, you will have seven minutes to present. Time will be strictly kept. I'll let you know when you have 30 seconds remaining, then

move on to the next speaker. Our first commenter for this morning will be Allison Adey. And -- oh, there she is. Allison?

MS. ADEY: Hi, can you hear me?

MS. HURTADO: Yes, we can hear you. You now have seven minutes.

MS. ADEY: Thank you very much. Good morning, I'm Allison Adey on behalf of the Personal Insurance Federation of California. We greatly appreciate the opportunity to participate in this pre-rulemaking session and provide some thoughts and comments regarding automated decision making.

The Personal Insurance Federation represents seven of the state's largest home and auto insurers. Our association deals exclusively in personal, property, and casualty lines. We believe it's important to understand that the insurance industry is already a highly regulated industry in general particularly on issues of privacy. The state's insurance commissioner heads the largest consumer protection agency in the United States with over 1,300 staff at a 300-million-dollar budget.

Current law provides the commissioner with unrestricted access to records, employees, officers, and contractors of any insurer. The commissioner is required to investigate the compliance of an insurer periodically,

but is permitted to examine an insurer at any time. Few industries have the routine presence of a regulator with the power of the insurance commissioner.

As it relates to automated decision making specifically, innovative technology has its benefits for businesses and is critical in industry such as insurance. ADM has a critical role in business facilitation using things like call routers, rating and underwriting decisions. If ADM is applied to the business of insurance, clarification is needed as to what is meant by the term if the CPPA were to participate as well.

For example, in the claims world, if certain medical bill processing software is deemed automated decision making and consumers have the right to opt out of that decision making, that could quickly become a problem and have an enormous operational impact. At a minimum, allowing opt-outs of that nature would delay claims handling time frames to the detriment of the claimant and compromise the insurers ability to timely comply with the various fair claims settlement practice regulations.

When the agency enters formal rulemaking, it will be very important to recognize current state and federal regulations that already regulate ADM to avoid duplication or conflicting regulation for insurers. Notably, the Gramm-Leach-Bliley Act, the Fair Credit

Reporting Act, and the Insurance Information and Privacy Protection Act.

ADM technology regulation should not impose any bans or purpose limitations on insurers use of artificial intelligence and machine learning, or to the extent that is not possible beyond what already exists under the existing privacy regimes. Should new regulations be appropriate within the framework of those laws, the enzo purpose limitation should not unduly burdened similar on insurance operations or efforts to innovate.

Additionally, we would point out that insurers or insurance related activities, such as rating, should be exempt from California's law defining profiling, including such activities and profiling may have a negative impact on the ability of insurers to deliver affordable products to California consumers. This is an area in which the California Department of Insurance already has oversight. For insurers the challenge of multiple regulators promulgating regulations, examining conduct, and taking enforcement actions is significant. With these preliminary insurance industry specific comments, we are hopeful that the agency will recognize the existing state and federal rules that insurers already comply with and that avoiding unnecessary and duplicative conflicting regulations will be a core

principle. Given the complexity and cost of compliance with CPPA and CPRA, our members also seek flexibility where possible and appropriate.

We look forward to working collaboratively with the agency and board to develop fair regulations that can be implemented in a manner that best serves Californians.

Again, we appreciate the opportunity to speak this morning on some of the aspects of our industry and the use of ADM there. Thank you so much for your time.

MS. HURTADO: Thank you for your comment, Allison.

Our next commenter will be Meredith Broussard.

Meredith, you now have seven minutes.

MS. BROUSSARD: All right, thank you. Hello, everybody. My name is Meredith Broussard. I am a data journalism professor at NYU, the research director at the NYU Alliance for Public Interest Technology, and the author of an upcoming book called "More than a Glitch, Confronting Race, Gender, and Ability Bias in Tech". Thank you for the opportunity to speak today. I'd like to speak about a few things we know about automated decision making and how we can make better automated decisions. In the Broadway musical Avenue Q there's a song called "Everyone's A Little Bit Racist". It's a parody song and it's quite rude, but I think the title is helpful to keep in mind when we're thinking about how

people make decisions. We all have unconscious bias. We are all working every day to become better people, but we are not yet perfect and we have bias and we often can't see it because it is unconscious bias. Let's let people imagine that if we turn decisions over to machines, to computers, the computers will make better decisions than people will. They think that the computers are unbiased or objective because what they do is based on math and this is itself a kind of bias. I call this bias, techno chauvinism. The idea that computer decisions are superior to human decisions.

Computer decisions are not perfect because people are not perfect. People imbed their own biases in the technology they create. Every computer program is written by people and every computer program has biases, which are the biases of the small, mostly homogeneous group of people writing the code.

So I propose a different way of looking at automated decisions. Acknowledging that a human only decision system is likely flawed because of bias and also acknowledging that a computer only decision-making system is likely flawed because of bias. Instead, the better path is humans and computers working together, as in most things.

We can use computational systems to analyze human

decisions and discover that, hey, black kids in New York City are not being admitted to selective high schools at the same rate as white kids and this is a problem that needs to be addressed. We can use human intelligence to look at the training data for GPT-3, the language generation model, and note that it is trained on data from Wikipedia, Reddit, and Hacker News, all of which have problems with sexism. With this in mind, we can predict that GPT-3 will generate sexist language.

We can use the lens that Ruha Benjamin offers in her book "Race after Technology", which is the idea that automated systems discriminate by default. When you start looking at automated systems through this lens, it becomes easier to spot problems. We have no shortage of evidence of bias and discrimination in automated systems. I wrote about some of them in my previous book, "Artificial Unintelligence"; I wrote about more of them in my upcoming book. We have Safiya Noble's book, "Algorithms of Oppression", which documents how google search results were racist until Google manually addressed the specific problems that Dr. Noble wrote about. Now, you don't get porn as the first google search result for black girls. It got -- it took decades to get that change made, however.

If we assume that automated systems discriminate by

default, we have an easier time developing standards and tasks that systems can be put through before being rolled out into the world. We can also look to the world of algorithmic auditing for methods of uncovering the bias that we know is inside these automated decision-making systems. Cathy O'Neil's company ORCAA does algorithm auditing, and they're developing a platform for evaluating algorithmic systems for bias. I'm very excited about the possibilities there.

There are also good mathematical methods that we have now for measuring bias, coming out of conferences like FAccT and NeurIPS. There isn't a good way to look inside the black box of an algorithm and explain what is happening because what is happening is very complicated math and it doesn't make sense to most people. This is a major challenge in writing regulations.

Regulators in every industry are going to have to become more computationally literate. A challenge that I think everyone is up to. Regulators should require companies to prove that their automated decision-making systems are not discriminating against groups based on protected characteristics before ruling out these decision-making systems.

The systems should be continuously monitored because code updates happen frequently and a system that passes

the bias test on Monday might be updated on Tuesday and might fail the bias test after the update. Companies should give up on techno chauvinism and make the difficult acknowledgement that their automated systems likely have problems because only by confronting the problem head-on, can we have any chance of fixing things. Thank you very much for the opportunity to comment.

MS. HURTADO: Thank you for your comment, Meredith.

Our next commenter will be Hilary Cain.

Hilary Cain, please raise your hand. Hilary, I'm going to go ahead and promote you to a panelist. You're able to use your camera if you wish. Hilary, you now have seven minutes. You may start any time.

MS. CAIN: Great. Good morning, my name is Hilary Cain. I'm vice-president for Technology Innovation and Mobility Policy at the Alliance for Automotive Innovation. I very much appreciate the opportunity to particulate in today's stakeholder session.

The Alliance for Automotive Innovation is the voice of the automotive industry in the United States focused on creating a cleaner, safer, and smarter transportation future. We represent the manufacturers that make up 98 percent of the U.S. new vehicle market, as well as automotive suppliers and technology companies working in the automotive space. The auto industry is the nation's

largest manufacturing sector responsible for more than 10 million jobs and representing 5.5 percent of the country's GDP.

Our member companies have long been responsible stewards of consumer information. In 2014, the auto industry came together to develop the privacy principles for vehicle technologies and services. The privacy principles, which are enforceable by the US Federal Trade Commission, represent a proactive and unified commitment by auto makers to protect identifiable information collected through in-vehicle technologies.

Through the development and implementation of the privacy principles, the auto industry has continued to gain significant insight into protecting consumer privacy while also advancing innovative automotive technologies that can help achieve important safety and environmental goals. We believe that the agency can and should accommodate the integration of cutting edge safety environmental technologies into modern vehicles as it works to fulfill its essential privacy mission. This is particularly irrelevant with respect to automated decision making.

The term automated decision making captures a broad range of use cases including automotive safety opportunities. For example, the artificial intelligence

that underpins next generation crash avoidance features and automated driving systems continuously makes real time automated decisions about what actions the vehicle will take to safely respond to and navigate the driving environment.

Automated decision making is also being integrated into occupant safety features that detect children who have been inadvertently left in a vehicle, or drivers who are inattentive or incapacitated. Allowing consumers to opt out of these sorts of automated safety technologies could have significant and likely unintended implications for motor vehicle safety not only for the consumer exercising his or her opt-out rights, but for other road users. At the same time, we contend that providing opt-out rights for these types of automotive safety use cases will not meaningfully improve consumer privacy.

As you are aware CPRA specifically mentions profiling as an area of automated decision making to be addressed by regulation. We recommend that the agency consider limiting the scope of automated decision making covered by the regulations to profiling. We further recommend that the agencies regulations only cover automated decision making that has significant economic or legal impact for a consumer such as decisions around housing, lending, education, or employment.

We also suggest that any right to request access to specific pieces of information related to automated decision making be restricted to personal information. In other words, if the information is not stored by the business in a way that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked directly or indirectly with a particular consumer, it should not be subject to an access request. This approach would be consistent with the access requirements elsewhere in the privacy law.

Before wrapping up, I wanted to touch quickly on one other issue. While we very much appreciate the interest in providing consumers with a right to correct and accurate personal information, we continue to have concerns about how this right can be effectively exercised with respect to vehicle generated data. Some of the data that is collected from vehicles is data generated by vehicle systems and components, including sensors. An accuracy challenge from a consumer related to this type of vehicle data is likely to create unnecessary and unresolvable challenges for vehicle or component manufactures. To that end, we suggest that the agency limit the right to request correction to personal information that has been provided directly by the consumer to the business to receive services.

Alternatively, we recommend that the agency allow businesses to deny a consumer's request to correct personal information if, for example, the consumer fails to provide sufficient information to investigate the accuracy of the challenged personal information.

Thank you again for the opportunity to present today. We look forward to continuing to work with you on these important issues.

MS. HURTADO: Thank you for your comment, Ms. Cain.

Our next speaker with be Jarrell Cook.

Can you please raise your hand Jarrell Cook? Jarrell Cook? Okay, we'll come back to Jarrell Cook.

Our next speaker will be Alyssa Doom.

Ms. Doom, I'm going to promote you to a panelist and you -- as soon as you move over -- you now have seven minutes.

MS. DOOM: Thank you. Good morning, Chair Urban and members of the California Privacy Protection Agency. Thank you for this opportunity to provide input on the upcoming rulemaking under the California Privacy Rights Act.

My name is Alyssa Doom and I'm speaking today on behalf of the Computer and Communications Industry Association or CCIA.

CCIA is a nonprofit, nonpartisan trade association

that for 50 years has represented a broad cross section of small, medium, and large technology firms. Our members place high value on the protections of individual privacy and support the important principles that underpin the CPRA, including transparency, accountability, and consumer control over how their data is processed and used.

CCIA has long supported the enactment of comprehensive federal baseline privacy legislation to avoid the creation of a divergent set of state privacy laws that could result in a confusing and burdensome regulatory patchwork. However, we understand that in the absence of a federal regime, state lawmakers have a continued interest in enacting local privacy policies to protect consumers. As such, CCIA has proposed a set of state privacy principles to inform legislators as local legislation is considered. Among these is the need to adopt a risk based approach to privacy protections. My brief comments will focus on the importance of adopting a risk based model for regulating the use of automated decision-making tools.

CCIA recommends that rules concerning ADM focus on securing protections for consumers with respect to decisions that are fully automated and that may have legal or similarly significant effects. The rules should

not create unnecessary restrictions for low risk systems and tools that support ordinary business operations and transactions. We advise that regulations involving ADM reflect the following principles governing regulatory terminology access to meaningful information and consumer opt-outs.

I'll first focus on regulatory terminology. The regulation of ADM is an emerging concept in privacy law and as such, the term lacks clear universally accepted legal definitions. Under the CPRA, the term automated decision making, could be interpreted so broadly as to encompass a range of low risk processing activities and basic tools that have proven beneficial for both businesses and consumers such as spreadsheets or spell checkers. The term could even reach the automated tools that digital services rely on to responsibly bronderate their services and keep users safe, such as chat, spam, and abuse filters. The adoption of overly inclusive regulatory terminology could impede the use of such widely accepted tools. Therefore, we recommend that regulations ensure that businesses shall only be obligated to implement access or opt out requests with respect to fully automated decisions involving personal information having legal or similarly significant effects, such as processing that impacts access to

medical treatment, public assistance, or credit decisions.

Next, I will turn to potential regulations governing consumers access to information about automated decision making. Again, CCIA recommends that the forthcoming regulations focus on high risk ADM processing. Here the agency should provide guidance on how to develop notices that contain simple and clear information regarding the purpose of the high risk automated processing and the source, categories, and relevance of the processed information. Companies should be able to make these disclosures through existing websites and transparency notices. Explanations should be straightforward allowing the users to understand the impacts of the ADM on their lives.

Importantly, the degree to which businesses will be required to disclose this information should be proportionate to the level of risk associated with the automated decisions and should not implicate trade secrets or business sensitive information. Disclosures should only be required in connection with automated decisions that produce legal or similarly significant effects for consumers. An obligation to provide disclosures for each type of low risk automated decision would overwhelm businesses and have no clear benefit to

consumers.

In addition, and equally important, regulations should not require businesses to disclose trade secrets or proprietary information such as algorithms or source code. These types of disclosures are unlikely to provide meaningful protections against risk or have little practical use to consumers and can severely chill not only the version of good customer service, but also innovation and speech.

Finally, consistent with emerging U.S. privacy regimes, only fully automated decisions that produce legal or similarly significant effects should be subject to rules establishing consumer opt out rights. To provide greater legal certainty, regulations should specify the categories of use cases that would be implicated here, such as decisions that result in the provision or denial of financial or lending services or access to essential goods or services. Broader applicability to lowerest decisions would impede ordinary business activity and diminish the availability and functionality of personalized consumer services.

Lastly, in instances where high risk ADM processing is essential to provide certain services or where a core function of the service is its automation, businesses should be able to demonstrate to consumer's supplemental

precautions taken instead of offering opt-out options.

In sum, requiring prescriptive one size fits all privacy controls that cover the processing of non-sensitive or De-identify data would be inconsistent with consumer expectations, degrade user experience, and hinder legitimate business practices. We believe the agency can mitigate these pitfalls while upholding privacy protections by promulgating regulations with these principles in mind.

CCIA welcomes the thoughtful and deliberative approach taken by the agency in considering the key operational enforcement issues introduced or modified by the CPRA. I'll also be submitting these remarks in a written format alongside the aforementioned privacy principals and invite members to contact me following the hearing should any questions arise. Thank you.

MS. HURTADO: Thank you for your comment, Ms. Doom.

Our next --

MR. SOUBLET: For our next speaker, I'd like to remind the panelists that when you're invited to speak, you may turn on your camera if you'd like.

MS. HURTADO: Thanks, Brian.

Our next speaker is Jarrell Cook. Go ahead and try him or her again.

Jarrell Cook, please raise your hand.

Okay. Let's go on to Dylan Hoffman, please raise your hand. Mr. Hoffman, I have promoted you to panelist. You may use your camera if you wish. And your seven minutes starts now.

MR. HOFFMAN: Thank you very much. Dylan Hoffman on behalf of TechNet. I'm the executive director for California here at TechNet. We're the bipartisan network of technology companies representing the innovation economy. Our members not only use ADS systems as employers, but many of our companies are also vendors in the space and so my comments will pertain to both perspectives.

I'll first start with a few general comments. Automated decision-making technology or ADS is not a universally defined term, and as noted by other panelists, could encompass a wide range of technology that has been broadly used for many decades including spreadsheets in nearly all forms of software. We caution against overly broad regulation of a broad category of technology that would impede the use of socially beneficial, low risk, and widely accepted tools to the significant detriment of both California consumers and businesses.

Everyday technology like calculators, word processing software, and even Scantron machines could be

considered ADS. Even newer and more complex ADS like artificial intelligence is used routinely in business and includes things like email spam filters and auto correct features. As currently defined in the CPRA, the term profiling is also quite broad. The definition arguably captures many low risk activities like movie recommendations on a video streaming service.

To the extent California is seeking to promulgate regulations related to ADS or profiling regulations under the CPRA, it is important to tailor any requirements to address specific known potential harms. The CPRA should apply a risk based standard for automated decision making that reflects the fact that the risk concerns and benefits differ across different use cases. For example, the impacts of solely automated decision-making systems and AI translation services can differ significantly from those in self-driving cars or AI medical software.

Regulations can be appropriately tailored to the risk by first applying only to fully automated decisions and second, applying only to decisions that have legally -- legal or similarly significant affects. If regulators are not thoughtful in crafting these definitions and corresponding requirements, it could limit the use of automated and algorithmic technology in California. For example, it would be unworkable for most

businesses to provide information to consumers on how and when a business's email spam filters make decisions to sort incoming messages. It would be equally unworkable for California businesses to accommodate individual consumer's requests to opt out of having their emails sorted.

I'd next like to address consumer access requests. Businesses should be able to fully fulfill consumer access requests and provide meaningful information about the logic involved in the decision by providing a general explanation of technology functionality, rather than information on specific decisions made. Providing a highly detailed explanation of the algorithms involved will not provide the average consumer with meaningful information on the logic involved and runs the risk of imposing obligations that conflict with the intellectual property, trade secret and other legal rights of the business in question. Any regulation should ensure that businesses are protected from disclosing propriety information such as that which is subject to an intellectual property or trade secret protection in response to consumer access requests.

Moving to the right to opt out. As I previously noted, automated technology has significant benefits for both businesses and consumers, including enhanced

accuracy and consistency, safer and more innovative products, and increased efficiency. Accordingly, regulators should be very mindful about providing consumers a broad right to opt out of (indiscernible) activities as it can severely hamper businesses and other consumer's ability to realize those advantages. If the agency chooses to pursue an opt-out, it should only be required for automated decision making including profiling when there is a decision made solely on an automated business basis and that decision produces legal or similarly significant effects concerning the consumer.

This aligns with the established standards in Virginia and Colorado laws, both of which provide an opt-out for profiling that's in furtherance of decisions that produce legal or similarly significant effects.

Finally, I'll close with a couple of considerations. First, regulators should not provide consumers erupt -- a right to opt out of low risk automated decision making as such a framework could be harmful to efficient business practices with little meaningful benefit to consumers. For example, imagine if consumers could opt out of a business using optical character recognition on PDF documents containing that consumer's personal information or if consumers could inform companies that they don't want their personal information stored in an internal

database that automatically sorts information alphabetically, but rather requires handwritten records be stored and sorted manually. Giving consumers the right to dictate how businesses use or don't use everyday technology can place a tremendous hardship on companies.

Second, to the extent that businesses are required to disclose use of ADS in high risk final decisions, consumers will already have the ability to opt out of automated decisions in those high risk scenarios by declining to do business with that company. Moreover, automation may be cored as certain high risk service offerings, making opt-outs infeasible. For example, an in car safety system that automatically senses a crash or immediately connects a driver with assistance shouldn't be required to provide a consumer with some sort of manual process that conducts the same task. That would defeat the purpose of the automated service. Limiting the regulation to only those high risk uses that have legal or similarly significant effects will help ensure that safety features in cars are not subject to unnecessary opt-out requirements.

To the extent covered by the definition of automated decision making or profiling ultimately adopted by the regulations, there should be appropriate carve outs for any processing related to fraud prevention, anti-money

laundering processes, screening, or for other type of security or compliance activities. Failure to do so would, for example, enable bad actors from opting out of automated processes that detects and blocks their fraudulent activities and limit company's ability to protect customer's privacy and security. Thank you.

MS. HURTADO: Thank you, Mr. Hoffman for your comment.

Our next commenter is Jarrell Cook. Jarrell Cook, would you please raise your hand? Give him a few seconds to respond. Jarrell Cook?

Okay. Commenter after that is Cathy O'Neil.

Cathy O'Neil, please raise your hand. Cathy O'Neil?

Okay. We will move on to Tatiana Rice. Tatiana Rice, please raise your hand. Thank you so much.

Ms. Rice, I will promote you to panelist. You have the option to use your camera if you wish. And your time begins now.

MS. RICE: Thank you to the California Privacy Protection Agency for initiating these stakeholder sessions and providing myself and others the opportunity to speak about issues regarding automated decision making, which undeniably will impact the future of consumer privacy and our ethical structure for technological development.

My name is Tatiana Rice and I am policy counsel at the Future of Privacy Forum. The Future of Privacy Forum is a nonprofit think tank based in Washington D.C. that focuses on consumer privacy and helping policy makers, privacy professionals, academics, and advocates around the world find consensus around responsible business practices for emerging technology. We believe that it is possible to build a world where technological innovation and privacy can coexist, which is why I am here today.

Today I have three specific policy recommendations for this agency relating to consumer rights of access for automated decision-making technology. First, that the agency should focus rulemaking on automated decision making as it relates to systems that produce legal or similarly significant effects on consumers. Second, the agency should ensure that access to information about systems are meaningful and reasonably understandable to the average consumer. And lastly, that the agency should consider ways to ensure that consumers rights of access and businesses' responses are inclusive and reflective of California's diverse population including those that are non-English speaking, differently abled, and lack consistent access to broadband.

So to my first point, the agency should establish guidelines for automated decision making that produce

legal or similarly significant effects. The term automated decision making encompasses almost every form of modern technology. This includes many routine, low risk practices such as loading a website, email filtering, or auto populating a form. Including such low level automated processing offers minimal, if any, benefits to consumers and risks unduly burdening businesses with invaluable tasks. However, there are some commercial automated decisions that do present serious risks to individuals, particularly in areas that affect an individual's civil and legal rights, such as hiring, housing, insurance, and lending. These systems are designed to recognize patterns and draw conclusions often using existing data and as a result, algorithms can then be trained on prior discrimination, like for instance, red lining practices with respect to housing.

When companies rely on biased algorithms to make important decisions they can unintentionally exacerbate existing inequalities and continue historical patterns of discrimination based on race, gender, sexual orientation, disability, and other protected characteristics. It's important to focus this agency's rulemaking on how consumers can gain a meaningful information regarding these higher risk systems.

In order to distinguish higher risk automated

decision making from the broader world of all technology that involves automation, a helpful guidepost would be to align the CPRA with Article 22 of the GDPR by applying heightened protections to automated decisions that lead to legal or similarly significant effects. The standard legal or similarly significant effects has the benefit of capturing high risk use cases while encouraging interoperability with global frameworks for which a growing amount of legal guidance is becoming available.

One key thing the agency may consider with systems that do produce legal or similarly significant effects include data protection impact assessments that identify benefits, mitigate risks to consumers, and identify and address any potential bias and discrimination in data sets, algorithms, and outcomes.

Second, information about automated decision systems should be meaningful and reasonably understandable to the average consumer. Explainability is a crucial principle for developing trustworthy automated systems. However, in practice it can be a challenge to provide truly meaningful explainable or interpretable AI for average consumers, particularly with more complex automated systems, such as neural networks and unsupervised machine learning.

In developing regulations on this topic, we

recommend that California follow best practices and guidance from the National Institute for Science and Technologies for principles of explainable artificial intelligence, which articulates principles for explainable AI systems; that the system produce an explanation, that the explanation be meaningful to humans, that the explanation reflects the systems processes accurately, and that the system expresses its knowledge limits.

What most consumers want to understand are the factors that led to a high impact decision and the main reasons for it. It's not enough to only provide what data is used and what the decision was, in order for that decision to be meaningful, a business would also likely need to share information about the relative salience or weight of each factor.

As noted in this guidance, the agency should also consider that meaningful is highly contextual and should be tailored to the audiences need, level of expertise, and relevancy to what they are interested in.

And lastly, but perhaps most importantly, the agency should ensure that consumer's right to access information about automated decision-making processes are inclusive and equitable. Consumer rights miss the mark if they do not afford all citizens the same opportunities and

rights. Data privacy rights are even more important to communities of color and immigrants who have long dealt with issues of over surveillance and systemic bias that pervades our technological systems.

According to the U.S. census, over 1.1 million households in California are limited English speaking, meaning all members 14 years or older have at least some difficulty with English. Though as common non-English language is spoken in these households are Spanish, Asian and Pacific Island languages.

Similarly, over 760,000 Californians have vision impairment and over 732,000 Californians do not own a computer. These factors do not stop entities from collecting data about them and using such data to make decisions. As a citizen of California, they should have the same ability to access this information as anyone else.

A few considerations to ensure equitable access of information to all consumers may include requiring entities to offer consumer access rights in other non-English languages, requiring web accessibility mechanisms and providing alternative processes for those without access to broadband to submit consumer access requests and receive responses through paper forms or other means.

The Future of Privacy Forum has published many

educational resources on automated decision making and we would be happy to continue working with the agency to provide smart and informative guidance regarding automated decision making and other topics. Thank you.

MS. HURTADO: Thank you for your comment, Ms. Rice.

Our next commenter will be Chris Riley.

Chris Riley, will you please raise your hand? Thank you. Okay. You now have seven minutes. Starts now. You may use your camera if you wish.

MR. RILEY: Thank you. Good morning, Chair Urban, Director Soltani, and members of the Privacy Protection Agency.

Thank you for setting up this process and inviting public participation in multiple stages along the way. I'm Chris Riley, senior fellow for Internet Governance at the Washington D.C. based R Street Institute joining you from my home in Concord, California.

The focus of my comments today will be about the intersection of automated decision making and internet governance. Whether we like it or not, automated decision-making technologies, or ADM's, I'll mostly refer to it, are the beating heart of the modern internet. So it's no real surprise they've received so much regulatory attention in recent years.

Now, while I understand and sympathize with the

motivation behind these interventions, it's just as important to map out the consequences of requirements such as those in the CPRA. Access provisions ought to provide information that is meaningful to the consumer, and contrary to some of the popular wisdom we're hearing on this topic, in most cases providing the algorithm isn't the right answer to that challenge. Similarly, opt-out rights to profiling based ADM feels right but has major consequences in practice particularly given the central role played by targeted advertising in the business models of companies both large and small.

It will cost substantial time and money for most companies to reach sustainability incorporating other business models, whether that's alongside targeted advertising or as an entire substitute, and not every company will survive that transition.

Now, I'm not raising these points to say the consequences outweigh the privacy benefits, nor to dismiss the obligation that CPPA has in practice to implement the relevant provisions of CPRA, which is law in California. Instead, I'm raising them to convey the opinion that we should approach the interpretation of the ADM obligations in CPRA, and all of them for that matter, with a long term frame of mind about what the future internet best ought to look like and then how we can

construct a glide path that gets us there successfully. The tasks specific to the question at hand and the relevant language of the CPRA represent a small, but in my opinion, very important part of that journey and that's why I'm here to talk to you today.

I want to add another important note of context, I think, in this exercise right now. These questions need to be looked at, not just alongside the GDPR and how that -- sorry, the General Data Protection Regulation and the EU just to be clear, and how the GDPR interprets similar language that it has regarding ADM. I know CPPA has already looked at that in depth. I've seen some of those materials; I'm really pleased to see that. We also now all need to think about this language alongside Europe's new Digital Services Act, also known as the DSA. We are still waiting on final texts for that law, but it has been agreed upon within the European Union and the press release that the EU issued says the bodies agree to include a requirement that large companies "will have to offer users a system for recommending content that is not based on their profiling."

In my mind, the DSA's decision to include this provision is very important in considering how broadly to scope ADM in the context of the CPRA and how to draw lines around the various intervention opportunities to

scope as tightly as possible the change you're trying to make as an agency. All of that is about increasing the likelihood of sustained success that you can have at the enforcement phase of this law.

A lot of the discussion in prior comment rounds of this process has focused on the scope of the ADM provisions, including a proposal to focus principally on ADM that has legal or similarly significant effects for consumers; we've already heard a lot about that this morning. I do think a focus like this would be practically helpful to the CPPA as it would ideally scope out the everyday use of recommender systems in search and social media and leave that territory to the digital services act and to Europe.

Honestly, I think it would be an enforcement nightmare to take that challenge on with the lean resources that you have available to you. I understand the value of filling gaps in federal activity in the U.S. There are a lot of gaps in federal activity in the U.S. on these matters. I also understand the principle at stake. The principle of providing an alternative to profiling based ADM is generally extensible to a large area of places in technology. I just believe that more practical benefit can be found in focusing the scope of ADM in the context of interpreting the CPRA into the more

tangible applications that are so often referenced, like mortgage systems and leaving the more general and more complex task associated with recommender systems and other sort of baseline internet programs to the DSA.

Okay. Onto access and process questions. As I said earlier, I believe show me the algorithm is practically meaningless in most cases. Machine learning uses fairly straightforward algorithms trained on massive corpuses of data attuned in practice through extensive testing and experimentation. What within that formula is most useful to a citizen, to a consumer to disclose? In my view, it's both sensitive and also arguably of limited utility to disclose the precise wanings involved in making a particular automated decision. These change so rapidly and are of limited explanatory value without a more total or systematic understanding.

Furthermore, any value that can be derived from that precise moment in time in waiting, can just as easily aide in gamification by spammers of (indiscernible). On the other hand, articulating the universe of factors that are taken into consideration in these algorithms could provide substantial value. The factors themselves, but not the precise waiting's provide healthy visibility to allow people to exercise choice by understanding the scope and the use of the data about them.

Ongoing improvement of ADM involves extensive internal AB testing on sets of users aggregated together. Now, there is value in such information as those AB tests in the context of things like the EU's Digital Service's Act, but in the context of access rights relevant to ADM for a specific individual, that kind of information feels beyond the scope. AB testing speaks more to collective rights and research issues, rather than anything on an individual level. And in general, I suggest, this may be a useful lens when considering the scope and nature of ADM and profiling in the context of CPRA, certainly for the internet and maybe more generally. Is the question, one fundamentally about an individual and what happens to them, in particular what happens in the context of their right to protect their privacy, or is it something more collective in nature, something tied to the responsibility of the platform in general? If it's louder, I suggest leaving it on the table for other regulatory frameworks to keep the CPPA focused on its mission --

MS. HURTADO: 30 seconds.

MR. RILEY: -- which is best -- thank you -- to deliver maximum impact with the resources it has. I was on my last sentence anyway. Thank you very much.

MR. HURTADO: Thank you for your comment, Mr. Riley.

Our next commenter will be Ridhi Shetty.

Will you please raise your hand? Okay. You now have seven minutes. You may use your camera if you wish.

MS. SHETTY: Thank you for the opportunity to speak before the California Privacy Protection Agency today. My name is Ridhi Shetty and I am a policy counsel at the Center for Democracy and Technology. CDT is a nonprofit nonpartisan 501-C3 organization based in DC that advocates for civil rights and civil liberties in the digital world. CDT works on many areas involving impacts of data practices in a public and private sector including privacy risks and inequities resulting from data driven or algorithmic decision making.

The California Privacy Rights Act requires the agency to issue regulations governing access and opt-out rights with respect to businesses use of automated decision-making technology including profiling and requiring businesses to respond to a consumer's access request by providing meaningful information about the logic involved in these systems and the likely outcomes these systems will have for that consumer. To this end, we call on the agency to ensure that the CPRA regulations address four points.

First, the CPRA regulation should explicitly articulate what automated decision making encompasses in

terms of both the system itself and the context in which it is used. The CPRA defines profiling, a related term, as the automated processing of a person's personal information to analyze or predict aspects concerning their performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements. The regulation should build on this definition by clarifying that there are two key aspects of the automated decision-making technology that are subject to regulation. One aspect is the design training data logic inputs and outputs of the methodologies involved in the automated decision-making system with a particular eye toward biases in those methodologies. For example, when racial, gender based, and or ablest biases are imbedded in an automated decision-making systems training data, the system can reproduce long standing inequities at scale and cause extensive harm to underrepresented and marginalized populations.

The other aspect is the overall context in which the automated decision-making system is deployed including the system's purpose and the ramifications of using a flawed system for that purpose, explainability of the systems design and function, and the manner and extent to which humans rely on the systems output to render any

particular final outcome related to a person.

Despite arguments that automated decision-making systems are less biased than human decision making, automated systems are far more limited in their ability to examine context and make nuanced decisions based on individual circumstances. Therefore, how and why the systems are deployed are just as important as the system's design, logic, and inputs and outputs.

Our second point is that the CPRA regulations should elaborate on substantive notice requirements so that consumers are empowered to hold automated decision-making systems and the businesses that deploy them accountable. Under the CPRA, notice to consumers must be easy for average consumers to understand and must be available in accessible formats for disabled consumers and in languages primarily used to interact with consumers. The CPRA regulations should further address the substance of these notices and elaborate on the explanation that consumers must receive about how their personal data is processed to produce a decision. Specifically, before subjecting consumers to an automated decision-making system, businesses should provide consumers with meaningful information about the logic involved in that process and its potential outcomes and their right to opt out of automated decision making. After using such

systems, businesses should also provide consumers with the principle reasons for any adverse decisions, data, or factors used to render such decisions and how the systems generated their outputs.

Third, the agencies rulemaking should pay particular attention to the impacts of discriminatory systems affecting critical areas of opportunity. Automated decision-making systems are playing a growing role in influencing hiring, compensation, promotion, and termination decisions in the workplace and labor market, limiting housing and credit eligibility, designating academic tracks, school intervention programs and disciplinary actions, and determining eligibility, budget locations, and potential fraud in public benefits.

Across these sectors, these systems are often trained to recreate ongoing decision-making patterns by evaluating a person against data from groups and subgroups that have benefited from historical discrimination. Even when those systems attempt to control for that bias, seemingly neutral data can function as proxies that lead to discriminatory impacts. All of this makes it considerably more difficult for historically marginalized groups to access critical life opportunities, yet the CPRA and the agency's invitation last fall for preliminary comments and proposed

rulemaking under the CPRA did not mention discriminatory harms of data practices. The regulation should address discriminatory outcomes explicitly because despite anti-discrimination protections, these systems have been used in ways that run afoul of civil rights and consumer protection laws with relative impunity. This is in large part due to the black box feature of automated decision making. One way to open the black box is through audit requirements.

The CPRA regulation should specify covered entity audit obligations particularly the frequency and substance of audits and make clear the agency intends to gather information and investigate equity impacts of automated decision-making systems.

And fourth, the CPRA regulation should preserve the existing exceptions under the California Consumer Privacy Act for governmental service providers. The definition of business under the CPRA is insufficiently specific to address the issue of businesses that provide services for public entities. Those businesses may be subject to CPRA's rights regarding access, disclosure, correction, and deletion. But requiring them to meet the CPRA's requirements may conflict with existing state and federal requirements for public entities regarding privacy, security, and public records.

Section 999.314(a) of the CCPA regulations rightfully classifies businesses that provide services to public entities as service providers, and requires them to collect, use, and delete data, only as directed by the government entity for whom they provide services.

This delineation of the duties of service providers is especially crucial for public schools because compliance with a CPRA's requirements for access, correction, or deletion, could cause unintended disruption to school services and student learning. In a similar vein, improperly scoped compliance requirements for businesses that provide services for agencies to administer government benefits may also delay or bar access to public benefits for those in greatest needs.

The exception for these businesses under the CCPA regulations helps avoid conflict with federal and state laws that could result from obligating service providers to disclose or compromise public data that the public entity is responsible for keeping secure.

I appreciate the agency's attention to these concerns, and the agency's efforts to strengthen California's regulatory framework with respect to automated decision making. I look forward to working with the agency, and I'm happy to provide further resource in expanding on these concerns. Thank you.

MS. HURTADO: Thank you for your comment, Ms. Shetty.

Our next commenter will be Carl Szabo.

Carl Szabo, please raise your hand.

Okay, we'll move on to the next one. Ben Winters, please raise your hand. Okay. Mr. Winters, I've promoted you. You may use your camera if you wish, and your time begins now. Mr. Winters, please unmute.

MR. WINTERS: My apologies. My name is Ben Winters. I am counsel at the electronic privacy information center. I'm lead of our AI and human rights project. Epic is a public interest research organization that fights for the protection of privacy and civil liberties. So I'm honored to be here today to talk about automated decision-making systems in the CPF (ph.). And so a lot is wrapped up and required to unpack in the sentence requiring the agency to issue regulations, governing access and opt-out rights with respect to business's use of automated decision-making technologies, requiring business's response to access requests. to include meaningful information about the logic, as well as the description of the likely outcome of the process with respect to the consumer.

So there, if we unpack a little bit, the agency has to define what automated decision-making technology is,

how access and opt-out rights must be actualized, what meaningful information about the logic involved actually means, and what a description of the likely outcome of the process with respect to the consumer means.

So those are really, really big sort of definitions that are really important for the way consumers and people are going to be able to be protected under this. And so Epic can recognize the enormity of this task and plans on following up with detailed written comments and suggestions but believes the definitions must be broad as to not leave out simpler systems that are not necessarily fully automated, or not necessarily using higher tech analysis. Because there is a lot of things that are not fully automated but has a sig -- substantial impact on individuals.

So one strong definition of automated decision-making systems that again we will provide in writing, was articulated by the scholar Rasheeda Richardson. And it defines automated decision-making systems as any tools, software system, process, function, program, method, model, and/or formula designed with or using computation to automate, analyze, aid, augment, and/or replace decisions, judgments, and/or policy implementations.

And so that definition, albeit not perfect, and although -- and -- and then there's no sort of perfect

definition that anyone's come across -- really recognizes the fact that you want to talk about the impact it has on people, not necessarily, like -- you can't really define every single system in a given definition. And I think that we recommend that you regulate based on (indiscernible).

And you can't just regulate based off of one sort of matrix. We recommend that you regulate on the sensitivity of data collected. So we're talking about, like, biometrics or personal information, personally identifiable information, the type of processing, whether it's being used for profiling, whether it's being used for facial recognition, analysis, or that type of thing. And the context. So whether it's used in hiring, in schooling, in sort of private criminal enter -- you know, justice investigations, then that -- those are three sort of independent, mutu -- not mutually exclusive contexts that should trigger a higher set of regulatory burdens.

And -- and to respond to concerns from industry about how an overinclusive definition would burden industry, I do think that, especially with access obligations, with opt-out obligations, you know, the -- the lift to provide meaningful information about that system should not be that high if it's not data collecting and processing a lot of personal information.

So I think that you have to really weigh the -- the meaningfulness of the protection versus, you know, potential regulatory burden.

So in regards to meaningful information about the logic, the CPPA should really require that companies, when any of these tiers are triggered, should require to explain in simple terms how different factors may impact a recommendation or a decision. And that's particularly important in the context of hiring, criminal justice, credit, and more. Because it just sort of goes into this black box, and -- and relatedly, that -- that goes to the sort of requirement that there's a description of likely outcome of the process with respect to the consumer.

In order for that to be meaningful, there needs to be substantial information that a consumer can trust. And so that should include at minimum, an understandable statement of what role the system is playing in the decision-making process, in -- in simple terms. So it should be able to say, we're collecting this information, which will output a numerical risk score between 1 and 10 based on X, Y, Z inputs, that will be changed by these sort of answers. Who -- which will then be provided to a loan officer that may use that number along with other factors to decide whether to offer you a loan. And so that's sort of one really clear way in a popup, you can

imagine, that we could actualize these rights.

But beyond that, there needs to be what the system is trying to predict, and the justification for why they're saying they can predict that. One huge problem we're seeing across all AI and automated decision-making systems is sort of the snake oil problem, where there are a lot of systems that say they can predict something, but that is not something they can predict, or it's not something that anyone can predict in some contexts. When we're talking about emotions, or predilections of -- of -- of various kinds.

And then beyond that they also need to give it a -- give a clear description of the output of the system, and the da -- how the data is going to be held or shared, and how consumers can request access deletion or opt out.

For those rights on access and opt out, I think that for the opt-out rights, there is -- we recognize there is a logistical challenge in certain contexts. And so I think that the opt-out rights shouldn't -- should be prioritized to be operationalized for those triggered risk tiers, based on, again, sensitivity of data collected, type of processing, and the context that it's being used in. And in regards to the access, they need to have, like, a sort of minimum available requirement of, you know, who created a system, who's being used, how

recently it's been validated, et cetera. And -- and one other thing I just wanted to respond to from earlier --

MS. HURTADO: Thirty second warning.

MR. WINTERS: -- is that -- great, thank you. Is that just because a given industry, whether it's being used in insurance, is highly regulated, doesn't mean it's well regulated, doesn't mean it's entirely regulated, and doesn't mean that with new regulations, there shouldn't be additional burdens that can protect people.

So again, thank you for the opportunity to talk, and we will be following up with written comments. And appreciate all --

MS. HURTADO: Thank you for your comment, Mr. Winters.

Mr. Winters was the last commenter for this session.

MR. SOUBLET: Sorry about that. I was having technical difficulties. We'd like to thank any -- everyone for the comments at this session. We ended a little ahead of schedule. We had several commenters who signed up and were not here this morning, so we're going to take a break now because we're on a schedule with people that have signed up to speak after the break. We'll take a break until our next session, which is on businesses' experiences with CPPA responsibilities. That session will begin at 12:30. Please feel free to leave

the video on or the teleconference open, or to log out now and back in at 12:30, when we will begin our next session. Thank you.

(Whereupon, a recess was held)

MS. HURTADO: Looks like we still have about four minutes.

(Pause)

MR. SOUBLET: Good afternoon. I'd like to welcome you back, or welcome you, if you weren't with us this morning, to the California Privacy Protection Agency's May 2022 Pre-Rulemaking Stakeholder Discussions. I'd like to remind everyone that we are recording. If you joined us this morning, this -- what I'm about to say, you may have heard already, but we want to make sure that everyone that's just joining us gets all of the information that we're providing.

I have some logistical announcements, and I will go over the plan for this session, which is our businesses' experiences with CPPA responsibilities session. As you can see from the programming schedule, which you can find on the meeting and events page on our website, we are holding a series of stakeholder sessions this week. Today, May 4th, May 5th, and May 6th. During the sessions, we will be hearing from stakeholders on a series of topics that are potentially relevant to the

upcoming rulemaking. Those who signed up to speak in advance were generally given a speaking slot for their first choice topic and will be limited to seven minutes.

We will proceed through the program according to the schedule provided on the website. Please note that all the times are approximate, and topics may start earlier or later than estimated. You are welcome to come and go from the Zoom conference as you'd like, but if you have an assigned topic, we recommend that you make sure you are signed in before your topic session begins.

Even if you did not sign up in advance, you will have an opportunity to speak during the time set aside for general public comment at the end of each day. Please take a moment to review the schedule to see when public comment is expected to occur. And again, please note that the times are approximate. Each speaker making general public comments will be limited to three minutes.

Please note that we will strictly keep time for all speakers in order to accommodate as many stakeholders as possible. We look forward to hearing from everyone, and it is important to note that stakeholders' views should not be taken as the views of the agency or the agency's board. They are the presenter's views only.

Speakers that are scheduled for the current session on businesses' experiences with CPPA responsibilities

should be signed into the public Zoom link using the name or pseudonym and email they provided when they signed up to request their speaking slot. If you are participating by phone, you will have already provided the phone number that you will be calling from so that we can call you during your pre-appointed speaking slot. Note that your name and phone number may be visible to the public during the live session and in our subsequent recording.

Speakers will be called in alphabetical order by the last name. During this window, we will not be able to wait if you miss your slot. When it is your turn, our moderator will call your name and invite you to speak. If you hear your name, please raise your hand when your name is called using the raise your hand function, which can be found in the reaction feature at the bottom of your Zoom screen. At that time, you may also activate your video as your -- your camera as you're presenting your comments.

Our moderator will then invite you to unmute yourself, and then you will have this seven minutes to provide your comments. In order to accommodate everyone, we will be strictly keeping time, as I mentioned. And speaking for a shorter length of time is just fine. When your comment is completed, the moderator will mute you.

Please pan -- plan to focus your initial comments on

your main topic. However, if you'd like to say something about other topics of interest at the end of your remarks, you're welcome to do so. You're also welcome to raise your hand during the portion at the end of each day set aside for general public comments.

Finally, you may also send us your comments via email or mail, and email them to regulations@cppa.ca.gov by Friday, May 6th, at 6 p.m.

Note, the California law requires that the CPPA refrain from using its prestige or influence to endorse or recommend any specific product or service. Consequently, during your presentation, we ask that you also refrain from recommending or endorsing any specific product or service.

I now ask that stakeholders who have been assigned to this topic to be ready to present. Please use the raise your hand function in Zoom when your name is called so that our moderator can easily see you. As noted, the moderator will call you in alphabetical order by last name. We will now move to the comments on the topic again of businesses' experiences with CPPA responsibilities.

Ms. Hurtado, could you please call the first speaker?

MS. HURTADO: Okay, thank you, Brian.

I'll be calling names in alphabetical order according to last name. If you're scheduled to speak in the session, you should have your hands raised already. Please do not raise your hands unless you've been confirmed. There will be a time during the public comment period at the end of each day for those wanting to make public comment.

When you have been called on -- when you have been called on, you will have seven minutes to present. Time will be strictly kept. I'll let you know when you have thirty seconds remaining, then move on to the next speaker.

And today, for this session, our first speaker is Amanda Anderson. Amanda Anderson, there you go. Can you raise your hand again, Amanda Anderson? Thank you. Okay, Amanda, I have promoted you to a panelist. When you're ready, you may speak, and unmute your camera and mic as you wish. Your time starts now.

MS. ANDERSON: Great. Good afternoon. My name is Amanda Anderson, and I'm the director of government relations at the 4A's. With these remarks today, I hope to leave you all with a better sense of the challenges in America's advertising agency's face when it comes to implementing the compliance requirements under the California Consumer Privacy Act.

The 4A's, also known as the American Association of Advertising Agencies, was established in 1917, to promote, advance, and defend the interest of member agencies, their employees, and the advertising and market -- marketing industries overall. Today, the organization serves more than 600 members across 1,200 offices and helps direct more than 85 percent of the total U.S. advertising spend.

4A's members are also significant employers in California, operating more than 198 member offices in the state. Advertising is a significant contributor to the U.S. economy. In August 2021, IHS Markit research report found that in 2020, advertising spend supported 1 -- 7.1 trillion in U.S. output, and 28.5 million U.S. jobs. The research also determined every dollar of ad spending supported on average over 21 dollars of economic output.

Collaborating closely with their nationwide and global advertiser clients, 4A's members are a critical part of the digital advertising ecosystem. Serving as the creative visionaries and business strategists behind how digital ads resonate and effectively reach California consumers. A strong advocate for common sense data privacy reform, the 4A's is an ardent supporter of federal -- the federal privacy for America policy framework, due to its emphasis on responsible industry

data use and self-regulatory enforcement, promotion of consumer choice, and built-in flexibility to allow the advertising industry to grow and innovate.

Agencies are likely to find themselves in a somewhat unique position when it comes to CCPA compliance. Under the law, a sale is not simply the exchange of California residents' personal information for money, but for a business value. A brand sharing a list of IP addresses to an agency to plant a targeted ad buy could be considered a sale under the law. As a result, compliance will often mean different things depending on the scope of the ad campaign being run.

Advertising agencies are required to evaluate each campaign by some specific data flows involved to understand how the CCPA might apply. It remains possible that an agency could be a business, a service provider, or a third party under the CCPA definitions in any given scenario, depending on the role they are playing. This can be costly, confusing, and time consuming to establish, particularly for small agencies, who have limited legal compliance resources, or data privacy management tools at their disposal, due to cost limitations. Even if not directly regulated as a business, under the CCPA, for specific data uses, agencies often serve as strategic advisors to clients in

complying with CCPA requests if such clients pass the request through to agencies.

Although agencies may serve as service providers under the CCPA in some instances, agencies deal -- that deal in California consumers' personal information are directly regulated as a business under the law. These covered agencies have needed to build compliance mechanisms to facilitate the required consumer privacy requests that the CCPA creates.

As a result, some agencies have established and maintained detailed processes for receiving and responding to consumer access deletion and opt-out requests. In the future, the CPRA will also require the agencies satisfy consumer data correction requests, requiring that additional processes be established to effectuate those consumer choices.

CPRA also requires that agencies properly train its employees to handle consumer inquiries about its or its client's privacy practices, CCPA requirements, and how to direct consumers to exercise their rights under the law. This requirement does not come without additional resource obligations, time commitments, and additional staffing costs.

In fact, a 2022 Gartner Research report suggests that businesses spend approximately 1,500 dollars to

process a single data subject request. The volume of data subject requests almost -- nearly doubled between 2020 and 2021, with the cost of processing them soaring to approximately 400,000 per million identities.

A standardized regulatory impact assessment of the CCPA estimated initial compliance costs for instate businesses alone at 55 billion dollars. The analysis also estimated 16.5 billion of additional direct compliance costs over the next decade.

Compliance costs also disproportionally affect small businesses. Small businesses with fewer than twenty employees would incur approximately 50,000 in initial costs, while medium businesses with employees between twenty and a hundred could incur an additional cost of 100,000 dollars. New data requirements in the CPRA will almost certainly increase privacy compliance costs from any agencies in 2023 if the CPRA closes the selling versus sharing loophole and clarifies that covered businesses must give California residents the option to opt out if their data is sold or shared with a third party for advertising purposes. This suggests that companies will see a considerable jump in the number of requests they receive.

Because no two businesses operate in the same way, we request that the agency provide flexibility to

businesses to respond to consumer data service requests. As such, we feel that rather than forcing businesses into explicitly defined procedures and processes, the agency and its enforcement mechanism should recognize self-serve tools that many companies and industry groups have already built to provide consumers the ability to exercise choice with respect to the use and disclosure of their information independent of any new requirements imposed by California's privacy law.

Similarly, the agency should better delineate its expectations for the businesses for when it receives a universal opt-out signal from a California resident but have an existing relationship with and/or consent from a consumer when it might conflict with that signal. Another serious concern for agencies in the years ahead will be the potential proliferation of fifty state different privacy and security statutes, each with its own -- each with its own unique compliance requirements. Harmonization with existing privacy laws is essential for minimizing costs of compliance and fostering similar consumer privacy rights to all Americans, no matter where they live.

To that point, a June 2022 information technology innovation foundation study, that small businesses like independent advertising agencies, would bear

approximately 20 to 23 billion of the out of state cost burden associated with multi-state privacy law compliance. The skyrocketing compliance costs could translate into a meaningful reduction in digital advertising spending and reduce revenues for agencies.

Digital media is a dominant and rising force in our economy. 4A's members are firmly committed to creating a world where consumers trust the media platforms and advertisers, and that they are -- and handling their data and offering ways to better engage with people in a way that they prefer.

On behalf of our members, the 4A respectfully requests that our comments and observations concerning CCPA compliance be included in -- in your consideration for the development of compliance requirements for the CPRA. Thank you very much.

MS. HURTADO: Thank you for your comment, Ms. Anderson.

Our next commenter in this session is Sheree Garner. Sheree Garner, please raise your hand. Sheree Garner?

Okay, we'll move onto the next person. Kate Goodloe? And I will go ahead and -- okay, Ms. Goodloe, I've moved you over to panelist. You may begin when you're ready, and you may unmute your camera if you wish. Your time starts now.

MS. GOODLOE: Good afternoon. Thanks for the opportunity to speak today. My name is Kate Goodloe. I'm a senior director of policy at BSA, The Software Alliance. BSA is a trade association of enterprise software companies. I often ask people to think of us as the B2B slice of the technology industry.

We have more than thirty global members, that include companies like IBM, Microsoft, SAP, Atlassian, Salesforce, and Workday, among others. Our members are global companies, and they compete to provide privacy protective products and services to other businesses. Things like cloud storage, workplace collaboration tools, and customer relationship management software.

Companies entrust some of their most sensitive information to BSA members, and our companies work hard to keep that trust. Their business models do not depend on monetizing users' personal information. I am on BSA's global policy term, and my whole job is to focus on privacy.

I'm especially glad to participate in this afternoon's session about the experience of businesses under the CCPA, because I want to highlight the different types of companies that are covered by the CCPA, which include not just businesses, but also service providers.

Under the CCPA, as -- as we all know, business is a

defined term. And it refers to companies that meet certain statutory thresholds, and that decide the purpose and means of processing consumers' personal information. In other words, businesses are the companies that decide how and why to collect a consumer's personal information. But the CCPA also applies to service providers. They're a separate set of companies with a different role. Service providers are the companies that handle data on behalf of businesses, and subject to specific limitations.

And because BSA members are enterprise software companies, they work for business customers, they're generally acting as service providers under CCPA. And of course, some of our companies will have consumer facing business lines, too. But the uniting feature of our members at BSA is that they offer enterprise services to business customers.

So today I want to focus on the role of service providers, and I'd like to make three points about their experiences under CCPA. The first -- and it's really hard to emphasize this enough -- is that the distinction between businesses and service providers is hugely important. That distinction is fundamental to privacy and data protection laws worldwide, which not only define these separate roles, but also put important obligations

on both types of companies. We've seen consensus globally for a while now that there should be obligations not only on the companies that decide how to collect and use consumer's data, which are businesses under CCPA, and often called controllers under other laws, but there should also be obligations on the companies that process data on behalf of other businesses, and pursuant to their instructions. Those are service providers, under CCPA, often called processors, under other laws.

So at the outset, I want to emphasize that our members appreciate the care that CCPA and CPRA take in recognizing these two distinct roles. Service providers are especially critical today as companies across all sorts of industries begin using digital tools and depend on other companies acting as service providers to store their data, connect them with customers and vendors worldwide, and help them collaborate across countries and offices.

So the second point I want to make is to stress that both types of companies, businesses and service providers, need to have strong obligations to safeguard consumers' personal information, and that's why privacy laws like the CCPA adopt obligations that reflect those different roles and that are tailored to them. Very often, laws and regulations are created by policymakers

that may be focused on specific business models, or specific practices such as ad-based business models, social media companies, or others. But of course, privacy laws can and should and do reach more broadly, to a whole range of companies that need to safeguard the consumer information that they manage.

Now the CCPA recognizes that service providers have important obligations to safeguard data, and those obligations are different from the obligations that are put onto businesses. For example, service providers are to enter into written contracts that limit how they can retain, use, and disclose the personal information that's provided to them by a business.

But the third point I want to make -- and this is really looking ahead to the upcoming rulemaking -- is to strongly encourage the CPPA to ensure that new regulations do not upset the relationship between business and service providers that is established under CCPA. And particularly, we recognize that the agency may issue regulations that address the ability of service providers to combine information that is received from different sources.

And as you look at that issue, we urge you to consider the wide range of circumstances in which service providers actually need to combine this information in

ways that have no -- nothing to do with monetizing the information or using it for advertising. In November, BSA submitted written comments to the agencies that included a half-dozen examples of scenarios in which service providers need to combine information that's received from different sources. These include routine activities, like securing a service that is offered to multiple business customers, identifying bad actors that may target multiple customer accounts, or improving the functionality of a service that is offered to multiple businesses, developing AI systems that test for bias across different data sets, or just serving two businesses that enter into a joint venture or a joint research project.

Fundamentally, service providers today don't work for just one business. They offer services at scale, which let companies across industry sectors use technologies like cloud computing and the video collaboration software we're on today. Providing, securing, and improving those services often depends on the ability to combine information that has been collected across business customers. And we urge you to keep those examples in mind as you begin the upcoming rulemaking.

Finally, I realize that time is short, but I'm

hoping to take the last minute of my time to briefly mention two other very important topics, which are cybersecurity audits, and risk assessments. Our members are global companies with extensive experience in both of those areas. And in both topics, we want to encourage the agency to leverage existing tools instead of starting from scratch. For cybersecurity audits, we recommend building on existing standards and best practices, especially the work of NIST and ISO. And we encourage you to recognize existing methods that companies can use to show that they comply with these leading --

MS. HURTADO: Thirty second warning.

MS. GOODLOE: All right. -- rather than creating a new set of requirements. And the same for risk assessments. We encourage you to look at the assessments required under other privacy laws and align California's requirements with those as much as possible to promote a harmonized approach to assessing risk and driving strong compliance practices. Thank you again for your time, and the opportunity to participate today.

MS. HURTADO: Thank you for your comment, Ms. Goodloe.

Our next speaker is going to be Sheree Garner. We'll go back to Sheree Garner, give her a chance to participate. Sheree Garner, can you raise your hand if

you're available?

We will go ahead and move on to Patrick Hedger (ph.). Patrick Hedger, if you're available, please raise your hand.

Okay, let's move onto the next person. Edward Holman? Edward Holman, please raise your hand. Thank you. Okay, Mr. Holman, I've promoted you to a panelist. You may use your camera if you wish. Your seven minutes starts now.

MR. HOLMAN: Thank you. Members of the board and agency staff, thank you for convening these pre-rulemaking stakeholder sessions and allowing me the opportunity to speak on today's important topics. My name is Eddie Holman, and I'm an attorney in the privacy and service -- security group with the law firm Wilson, Sonsini, Goodrich, and Rosati, based in the firm San Francisco office.

My ideas expressed today reflect my personal experience as a licensed attorney in the state representing businesses in connection with their CCPA compliance activities, but do not necessarily represent the views of any particular client or my firm. I would however like to draw the agency's attention to the preliminary written comments submitted by my firm on November 8th, which I coauthored with one of my

colleagues, Tracy Shapiro.

Given the brief amount of time I have available, I'd like to highlight a few of the issues from that written submission in the context of the topic at hand for this session. First issue I'd like to highlight is harmonization. Many businesses have invested significant resources in complying with the CCPA, typically in addition to resources already spent on compliance with the GDPR and other applicable privacy laws.

Now in addition to the changes the CPRA makes to the CCPA, businesses are trying to figure out how to harmonize compliance with other state privacy laws that have emerged in Virginia, Colorado, Utah, and most recently, Connecticut. Subtle but significant differences among these laws have already created challenges for companies trying to update their CCPA compliance activities. In particular, the emerging state privacy laws have often different definitions of important terms, different requirements around certain consumer rights, and other different compliance obligations that do not closely align with the CPRA. In the interest of both consistency for consumers and efficiency for businesses, I encourage the agency to look outward and seek to harmonize the CPRA's compliance obligations with those of other privacy laws where

possible.

The second issue I'd like to highlight is that of contracting with service providers. As I think we just heard, the CCPA requires businesses to impose certain restrictions via contracts with service providers. Because of the differences in similar obligations under other privacy laws, this has not been a straightforward activity. It typic -- typically requires many hours of locating, renegotiating, and amending existing agreements. The CPRA's new requirements for agreements with service providers and contractors is requiring businesses to revisit this burdensome process. Compounding this issue is that many of the CPRA's new requirements do not map neatly onto new requirements in other emerging state privacy laws.

There are two key issues causing complications that I'd like to highlight. First, section 1798.100(d) of the CPRA requires businesses to enter into agreements with all parties with whom they disclose personal information. It is unclear, however, whether this requirement applies to onward transfers by the other party, particularly as between the business's service providers and the service provider's subcontractors. The agency should clarify that the CPRA permits businesses to comply with this requirement by requiring service providers and

contractors to flow down the required terms to their subcontractors.

Second, existing CCPA regulations permit a service provider to retain, use, and disclose personal information obtained in the course of providing services, "to detect data security incidents, or protect against fraudulent or illegal activity". This is a critical exemption relied upon by companies that provide vital cybersecurity and fraud prevention services, and it is important that it be preserved in the CPRA regulations.

Third issue I'd like to highlight is behavioral advertising. A frequently and hotly debated topic under the CCPRA -- and under the CCPA has been whether the disclosion -- disclosure of certain types of data for advertising purposes constitutes a "sale under the CCPA". As the agency may already be aware, there are numerous types of online advertising, not all of which fall neatly into the common buckets of contextual advertising on the one hand, and advertising based on building profiles using data collected across different services over time on the other.

For example, different types of ad retargeting, the use of first or third-party advertising, inclusion, or exclusion lists, and the use of look-alike audiences to target ads to similar consumers all raise questions about

their appropriate classification. CPRA is causing masy -- many businesses to have to revisit questions regarding which of these advertising activities can be performed by service providers, and which will require offering opt-outs.

Both businesses and consumers would benefit from more granular guidance from the agency regarding what advertising activities constitute a "sale" or "sharing" under the CPRA. Without this additional clarification, businesses will inevitably interpret this language differently from one another, creating unnecessary compliance risks and resulting in inconsistent treatment for consumers exercising their right to opt out.

The final issue I'd like to highlight, are really two issues regarding global opt-out preference signals. First, section 999.315I of the existing CCPR regulations, which requires businesses to honor certain types of user-enabled global privacy controls, is plainly inconsistent with the regulatory authority of this agency under Section 1798.185(a)(19) of the CPRA already in effect.

Inconsistencies between the law and regulation cause unnecessary expenditure of resources by businesses, and confusion on the part of consumers as to the promoted efficacy of certain opt-out tools. To address this issue, ti -- the agency should promptly repeal Section

999.315(c) of the existing CCPR regulations until it can be replaced with new regulations for an optional opt-out preferice -- preference signal that is consistent with the CPRA's requirements.

Second, many advertisers and publishers are unfortunately forced to constantly combat fraud in the online advertising industry, global losses estimated to run in the billions of dollars annually. This fraud increases advertising costs, which ultimately results in increased costs for consumers. It is therefore crucial that businesses be permitted to scan for and defend themselves against such fraudulent activity, including where such activity seeks to exploit opt-out preference signals, possibly to -- in an attempt to evade detection.

Emerging privacy laws in Colorado and Connecticut expressly contemplate that businesses be allowed to accurately authenticate the consumer using such an opt-out as a state resident and determine that the mechanism represents a legitimate request to opt out. The agency should incorporate the same authentication permission into the CPRA regulations.

Thank you for your time, and I look forward to future participation in the rulemaking proceedings.

MS. HURTADO: Thank you, Mr. Holman, for your comment.

Our next commenter will be John Kabateck. Thank you. Okay, Mr. Kabateck, I have -- Mr. Kabateck, you may use your camera, and your time starts now.

MR. KABATECK: Okay. Well thank you very much. And thank you and good afternoon committee members. I really appreciate the opportunity to be here. My name is John Kabateck. I am the California state director of the National Federation of Independent Business. I am here on behalf of NFIB representing our small and independent business owner members in California, but also the nearly sixty additional small and medium-sized business groups and associations that we have been working together with on privacy and other important state issues. I appreciate being here; thank you for the opportunity to provide comments on the businesses' experiences, to date, with CCPA responsibilities.

I'd like to quickly just raise four significant issues for the agency and board to consider in its deliberations on the issue that are raised in these and future meetings regarding the confusing, onerous, costly, and complex nature of California data privacy laws and regulations. First, new data privacy research published by CYTRIO last week revealed that 90 percent of companies remain unprepared for the California Consumer Privacy Act of 2018, and the European Union requirements, and general

data protection regulation, end of quote.

They had research confirming the privacy rights management solutions have not gained wide adoption due to cost and deployment complexity, resulting in a high percentage of CCPA noncompliance. Quite frankly, it's difficult to find fault with these companies when the state has changed the laws and regulations around privacy so many times. There are very few business organizations that understand highly technical mandates, and the requirements, and little resources to inform them of measures required to comply. Most businesses, it's important to point out, are so confused about whether they will be unable to comply with the requirements that currently exist, much less any new regulations that might be imposed.

My second point, the privacy policies that already exist have added another layer of onerous regulations during a time when our members are trying to regain their footing and manage uncertainties related to the pandemic. According to the Public Policy Institute of California, "very small businesses are more likely to be owned by women and nonwhite Californians, making matters worse for small businesses". Many people who have jobs aren't returning to their urban offices full time, or staying home. So many small businesses that relied on these

employees being at work and buying things from them have little or no customers. And imposing further regulations when our small businesses are still recovering only worsened the business conditions.

Third, we urge the CCPA to support our businesses and refrain from setting up a punitive system that encourages fines, penalties, lawsuits. Businesses are well intentioned and want to be in compliance with the laws and regulations, but they need resources that can empower them rather than open the door for further threats to the existence of their businesses.

And lastly, small and medium-sizes businesses need the low cost and at times free digital tools, resources, and marketing challenges that are now available to compete with large businesses. If the new privacy laws impose costly burdens, it's going to be small business owners who bear the brunt of these new costs and operational issues.

According to an economic impact assessment study prepared for the attorney general's office, the total cost of compliance for the CCPA alone would be approximately 55 billion dollars. And today, as we observe the board beginning the rulemaking process for CCP -- CPRA, the California Privacy Rights Act, we do anticipate that this figure will only become more costly

for our businesses.

So in closing, committee members, we understand the CPPA is an attempt to create a new privacy standard for the world, and we appreciate that, but we do ask that the academic review of the state's privacy policy also for sure include a practical evaluation of the unintended consequences and impact that this -- that could result in higher business costs, lost jobs, and businesses failures.

Thank you so very much for your time.

MS. HURTADO: Thank you for your comment, Mr. Kabateck.

Our next speaker will be Andrew Kingman. Mr. Kingman, when you're ready, you may turn your camera on if you wish. And your time will start now.

MR. KINGMAN: Hi, good afternoon, everyone. Thank you very much for your time today. My name is Andrew Kingman; I'm an attorney in DLA Pipers Data Privacy and Cybersecurity Practice Group. As other have said, my views today are my own and -- and don't represent the views of any particular client.

In the context of businesses' experiences with implementing CCPA, I'd like to talk about process, unintended consequences, and ambiguities that have arisen. And first, I want to acknowledge some helpful

outcomes from the lot. And from the AG's office, the CCPA, along with the GDPR has catalyzed many businesses to take stock of their data mapping in a more robust manner. And second, the attorney general's office has issued a report detailing its enforcement actions, particularly around the right to cure efficacy, that has been useful in understanding enforcement priorities.

Lastly, it has built a tool to allow consumers to submit right to cure notices for opt-outs through the AG's website, which is a helpful step in facilitating consumer involvement. I also want to state clearly that the vast, overwhelming majority of businesses genuinely want to comply with this statute. They want to ensure that their customers have the best possible experience; they want to avoid data security incidents. They want to make sure that their vendors can get the job done right and respect the consumer's privacy at the right time.

The experiences that I speak to today are offered as a realistic accounting of what businesses' experiences have been, and are offered in good faith to help strengthen this process moving forward.

So the first thing I'd like to talk about again is process. So we're -- we're coming up on four years since the CCPA's passage, and since then there have been five amendments enacted, four drafts of regulation, the CPRA,

additional rulemaking, and we're looking at at least seven bills in the current biannual that would amend the CPRA or CCPA.

So there's a lot of frustration on -- on business's sta -- from business's viewpoints, that, you know, as a result of this, certain enforcement deadlines or rulemaking deadlines have slipped, and -- and that's understandable given -- given the process here. But also, you know, businesses are a little bit frustrated that there hasn't been a recognition of that with compliance expectations. So the result of this is that businesses have been put in a position of devoting resources to implementing provisions that may change, and therefore wasting time and money, or delaying implementation in order to ensure that they know exactly how the statutes and regulations fit together. So as this body goes forward with its rulemaking, we would encourage recognition that businesses want to comply, but that they want to be able to have the certainty of knowing where things stand.

The second -- just a couple examples of unintended consequences in the implementation here. The first is with the privacy policy, and the various notices that are required by both the CCPA, the regulations, and -- and the CPRA here. I think businesses are frustrated because

there's always a tension in privacy between comprehensibility for nonexperts and being fulsome and transparent in -- in a business's activities here. I think businesses can be frustrated, because meeting all of the statu -- statutory and regulatory requirements here often means sacrificing readability and accessibility. And that, of course, is the entire point of a privacy policy.

And so being able to simplify some of the requirements in these notices, potentially reducing the number of notices, I think, would be something that would be very welcomed by the business community, and I think doing that would actually increase meaningful consumer privacy moving forward.

The other -- the other issue in terms of unintended consequences would be the definition of sale. And interpreted broadly, this in some cases requires business to business entities that have public websites that are not designed for consumers, per se, but for their customers, but the pub -- the public can visit. Those websites, with any free cookies, analytics, things like that, they're required to put up do not sell links and adopt a posture as a controller only with regard to their website.

And -- and any guidance or clarification around

this, I think, would be helpful. Certainly would concur with prior comments around service providers having to be controllers in some -- in some cases and not others. But this per -- this example in particular is very frustrating because it requires service providers to state that they are selling consumer data. In general, they are not doing any activity that would generally be thought of as -- as a sale.

The last piece I wanted to address is just ambiguities in the statute. And again, a couple examples here that I wanted to raise. One specifically around the global privacy control. Again, this has already been flagged, but you know, the rules from the CCPA clearly contemplate a global privacy control or universal opt-out mechanism, but do not lay out any specifications.

There have also been communications from the attorney general's office that it is mandatory to recognize those signal -- signals. However, the CPRA quite clearly makes that recognition of signals optional, and so these types of conflicts and ambiguities make it very difficult to -- to give businesses the peace of mind that they are, in fact, in compliance.

Lastly, in the CPA, there's the new term of contractor. In its usage, when compared with a service provider, it's not very clear, given that they are very

similar in definitions. And so any guidance on what circumstances a contractor -- an entity would be classified as a contractor and not a service provider would be very, very helpful.

In my final few seconds here, I would simply like to address the concept of automated processing and encourage this -- this body to be -- to adopt the idea of automated processing in a somewhat narrow view that -- that would be solely automated processing, simply because activities that involve both automated processing and human review comprise virtually every type of automated processing. I think this subverts the intent of the idea of -- of profiling and automated processing, and would request that --

MS. HURTADO: Time, Mr. Kingman.

MR. KINGMAN: -- the body move -- yep. And would just request that the body move incrementally in interpreting that. Thank you.

MS. HURTADO: Thank you for your comment, Mr. Kingman.

Our next speaker will be Peter Leroe-Munoz. Mr. Leroe-Munoz, thank you. Mr. Leroe-Munoz, when you're ready. Okay, I see you're ready. Your time starts now. Feel free to use your camera.

MR. LEROE-MUNOZ: Very good, thank you all very

much. Much appreciated. My name is Peter Leroe-Munoz. I'm the general counsel and senior vice president of technology and innovation for the Silicon Valley Leadership Group.

Approximately 60 percent of our member companies are direct technology companies. That is, a -- a diversity of companies ranging from software and consumer devices to nanotech, semiconductors, clean tech, and beyond. The balance of our membership includes a variety of industries that support our technology core. We have members that represent financial and professional services, healthcare, higher education, and more.

And our membership also includes businesses of all sizes, as well as most of the large brands in Silicon Valley. Now the leadership group is hundreds of employer members in the broader Silicon Valley region. And on behalf of our members, I'd like to thank the CPPA board for the opportunity to share my comments today regarding the businesses' experiences to date with CPPA responsibilities and cybersecurity audits, and risk assessments performed by businesses.

In the past few years, data privacy laws and regulations have emerged across the country. And while our members understand that it is a high priority to protect consumer data, the manner in which the policies

have been passed have lacked harmonization, and creating an extremely challenging legislative and regulatory environment for businesses that are looking to comply.

In a January report by Information Technology and Innovation Foundation, ITIF, a nonprofit, nonpartisan research and educational institute, finds that since 2018, thirty-four states have passed or introduced seventy-two privacy bills, regulating the commercial collection and use of personal data. Many California businesses operate outside the state lines, which means they are subject to a myriad of privacy policies, not to mention an additional layer of privacy mandates specific to certain industries, such as the financial sector that have been in place for years.

There should be a consistent standard for assessing what constitutes a significant risk across state lines, to allow for businesses to continue to build robust processes to protect consumers' information. Now needless to say, businesses' experience with CCPA responsibilities have not always been easy. Examples of compliance measures that create operational and cost concerns include actions such as hiring technical staff, purchasing systems to build and maintain information, training and managing staff, and ongoing maintenance to ensure compliance with out-of-state policies.

As it relates to cybersecurity audits and risk assessments performed by businesses, we highly encourage the board to ensure these items are confidential to invoid -- to avoid revealing trade secrets and avoid the potential for phishing expeditions. The audits and assessments should only be conducted on a specific risk or issue. If not, this could open the floodgates for fraud and security breaches and dissuade businesses from taking further compliance action for fear that it would threaten the existence of their business.

We are concerned that all of these costly and burdensome privacy provisions, and very little resources information are available to support businesses' good faith efforts to comply, will ultimately lead to negatively impacting businesses, that will have a ripple effect of unintended consequences -- consequences, such as lower worker productivity, reduced economic -- reduced economic activity, and limitations on innovation in California.

My thanks to you for receiving our comments this afternoon.

MS. HURTADO: Thank you very much for your comment, Mr. Leroe-Munoz.

The next commenter will be Clark Rector. And in just one moment, let me move him over. Okay, Mr. Rector.

Okay, your time starts now. You may use your camera if you wish.

MR. RECTOR: Very good. Well thank you for the opportunity to address you today. My name is Clark Rector. I'm the executive vice president of government affairs for the American Advertising Federation. The AAF is the umbrella association for the advertising industry. Our corporate membership includes many major advertisers, advertising agencies, and the media, including print, broadcast, outdoor, and online media. We also represent over 35,000 advertising professional -- professionals in 150 local advertising federations across the company, including ten California advertising associations.

A significant portion of these local members are from small businesses. And it's primarily their concerns I'd like to address today, as well as giving the agency a reminder of the context in which all of these regulations exist.

Now like you, the AAF supports providing California consumers with appropriate notice of businesses, data practices, and the ability of those consumers to exercise effective choices. While the primary focus of this is business experiences to date with the CCPA responsibilities, for many of my members, quite frankly, they're experience is still somewhat speculative as they

don't always reach thresholds of compliance, but it's of course always these goals to -- their goal to -- to stay within compliance and grow so that they do meet all these obligations.

It's important to remember that moving forward the importance of the internet economy and the responsible use of data to the overall economy. Since 2016, the internet economy's contribution to U.S. GDP has grown 22 percent per year. In 2020, the internet economy contributed 2.4 trillion to U.S. GDP and more than 11 percent the total and eight times what it was in 2008.

In 2020, the commercial internet generated more than 17 million U.S. jobs, and it's important to remember that of those jobs, more of them actually came in small businesses than in the largest internet companies, and all of this is made response -- made possible by the responsible use of data.

In addition to fueling economic growth, responsible data-driven advertising subsidizes the measure amounts -- immeasurable amounts of free and low-cost news and entertainment. Advertising revenue is important and often the primary source of revenue for online publishers, and decreased advertising would also result not just in lower profits for digital publishers, but less content for consumers.

A survey conducted for the Digital Advertising Alliance showed that 90 percent of consumers stated free content was important to the overall value of the internet, and 85 percent prefer the existing free ad supported model over having to pay for content. Surveys show that more than half of consumers prefer the relevant ads, and certainly the ability for small businesses to responsibly serve interest-based advertising, more likely consumers, allows them to punch above their wake and compete with much larger businesses.

Responsible businesses recognize that consumer trust is paramount in growing their business. Lost trust is not easily recovered, be it in data practices or any other area. My members want to be able to do the right things for themselves and for consumers, but their small size also means they have fewer resources, and despite best intentions, sometimes a limited ability to ensure compliance.

One of the biggest challenges for -- challenges for businesses of any size, but particularly small businesses, is the border-free reality of the internet. Consumers often do not know where an online business is located, California or otherwise. Likewise, on the internet, a California business is open to consumers all across the country and much of the world. As a previous

speaker has said, there are numerous privacy laws out there in other states, and businesses need to be able to con -- to comply with all of those. Virginia, Colorado, Utah, recently Connecticut have all passed privacy bills.

So to the extent possible, we would ask that the agency work to harmonize requirements and terminology with that of other states. Harmonization would ease burdens on businesses, especially the small businesses, increase compliance, and lower costs, and it would also benefit consumers by minimizing confusion about different rights and protections from state to state.

Again, I appreciate the opportunity to be able to address you today and recognize the challenges of the task before you. Thank you for hearing our concerns. The AAF looks forward to working with you as the rule-making process advances.

MS. HURTADO: Thank you so much for your comment, Mr. Rector.

Our next commenter will be Kevin and David. Okay. Mr. Walsh.

MR. WALSH: Good afternoon.

MS. HURTADO: Your time starts now.

MR. WALSH: Thank you. Thanks. David Levine is not with us today. It was just easier to do one person calling in.

Members of the Board and -- and agency, thank you for these hearings. I'm Kevin Walsh. I'm a principal at Groom Law Group, an employee benefits firm based in Washington, D.C. I'm here today on behalf of the SPARK Institute. SPARK represents the record keepers of retirement plans broadly. SPARK supports the mission of CCPA and the CPRA to provide individuals with the privacy rights that they expect. And thank you for having us here with the experience of businesses that we represent have had to date.

So you know, so far the employee/employer and the B2B specific roles have largely prevented conflict between the goals of employees and employers and privacy goals of California, and you know, as additional states have acted, for example, Virginia, Colorado, Utah, and Connecticut, they have all recognized that employment-related benefits are unique, and you know, unique privacy rules are needed to ensure that employees continue to get those benefits.

And you know, so we're here basically to say that it's important that harmony continues and that new regulations not interfere with the ability of employers to provide the benefit employees expect. So CPRA had a two-year extension of the employee and B2B specific provisions, and right now the assembly is concerning

legislation that would further extend those (audio interference) proactively. So how do you (audio interference) special rules (audio interference) --

MS. HURTADO: Mr. Walsh.

MR. WALSH: -- broadly.

MS. HURTADO: Mr. Walsh, you're breaking up quite a bit.

MR. WALSH: Okay. I'm sorry. Okay. Is this -- is this better?

MS. HURTADO: Yeah. It seems a bit better, yes.

MR. WALSH: Is it? Okay. So I'll be -- I'll be quick. So first off is that, you know, if -- if rules stand, it's likely that employee/employer relationships are going to need unique rules, so putting in rules that would snap into effect should the -- should the employee provisions not be extended this year, will likely just lead to increased compliance costs because it's likely that the legislature will act or that -- that we'll need to regulate a way, again, to ensure that employee can get the benefits they expect.

Second, regulations should make clear that data use is permitted to the extent it's reasonably related to providing employees with benefits, and benefits should be defined broadly. So good services the employee receives access to by virtue of their relationship as the employee

of an employer.

A broad definition is vital. If you look back ten years, very few employers provided financial wellness or provided access to programs in helping pay down student loan debt. So any definition that's used today should be future-proofed to make sure California residents get access to the same innovative benefits that employees get elsewhere.

And lastly, I just want to highlight real briefly why special rules are needed, and just look -- look at the operation for retirement plans. If participants can't be found, then saving for retirement or having access to a pension is really a waste of time. So optouts and controls for a 401(k) plan, they -- they really can't work.

So if you look at ERISA, which is the statute at the federal level that governs these plans, there's no specific provision that says you've got to, you know, find everyone. But if you talk with the labor department, if you worked with planned fiduciaries, planned sponsors, they need to be gathering data about employees, their email addresses, their contact information, their -- their (indiscernible) beneficiaries; otherwise, you know, they can't provide the benefits they -- they -- they are promising by law to

provide, and similarly our right deletion or further opt-outs and controls would cause similar concerns.

So I mean, those are the three points I wanted to make. I want to thank you for your time and say that SPARK looks forward to working with you as the rule-making advances.

MR. SOUBLET: Mr. Walsh, some of your comment was interrupted by the interference. If you wouldn't mind, if you have them written, can you submit them to us to regulations@cppa.ca.gov, G-O-V --

MR. WALSH: I'd be happy to.

MR. SOUBLET: -- so that we make sure we have everything that you wanted to say.

MR. WALSH: All right. Thank you. I will definitely send those to you.

MR. SOUBLET: Thank you. Thank you again, everyone, for your comments. This is the end of our session on business experiences with CPPA responsibilities. We have another session that is set to start at 3:00. So we're going to take a break again. Please feel free to leave your video or teleconference open or to log out now and back in when we start that session that begins at 3:00, and that is on consumers' experiences with CPPA rights. Thank you.

(Whereupon, a recess was held)

MR. SOUBLET: Good afternoon. It's now 3:00. I'd like to welcome you to the California Privacy Protection Agency's May 2022 Pre-Rulemaking Stakeholder Sessions. I'd like to remind everyone that we are recording.

Before we start this afternoon's session, we noticed that there were some hands raised during the last session. As a reminder, the sessions are scheduled for speakers that previously registered to speak on a specific topic. Those that have raised their hands that are not on the schedule, if you'd like to make general comments, we have set time aside at the end of each day for a public comment period.

As mentioned before in our earlier sessions, I have some logistical announcements, and I will go over the plan for this session. As you can see from the program and schedule, which you can find on the meetings and events page of our website, we are holding a series of stakeholder sessions this week, May 4th, 5th, and 6th. During the sessions, we will be hearing from stakeholders on a series of topics that are potentially relevant to the upcoming rule-making. Those who signed up to speak in advance were generally given a speaking slot for their first choice topic time and will be limited to seven minutes.

We will proceed through the program according to the

schedule provided on the website. We look forward to hearing from everyone. It is important to note that stakeholders' views should not be taken as the views of the agency or the agency's board. They are the presenter's views only.

Speakers that had scheduled for the consumers' experience with the CCPA responsibilities session should be signed into the public Zoom link using the name or the pseudonym and email that they provided when they signed up to request their speaking slot. If you are participating by phone, you will have already provided the phone number that you will be calling from so that we may call you during your pre-appointed speaking slot.

Note that your name and phone number may be visible to the public during the live session and subsequent recording. Speakers will be called in alphabetical order by last name during this window, and we will not be able to wait if you miss your slot. When it's your turn, our moderator will call your name and invite you to speak, and if you would like, turn on your camera.

If you hear your name, please raise your hand when your name is called using the raise your hand function, which can be found in the reaction feature on the bottom of your Zoom screen. Our moderator will then invite you to unmute yourself, and then you will have seven minutes

to provide your comments.

In order to accommodate everyone, we will be strictly keeping time and speaking for shorter length of time is just fine. When your comment is completed, the moderator will mute you. Please plan to focus your remarks on your main topic; however, if you'd like to say something about other topics of interest at the end of your remarks, you're welcome to do so. You're also welcome to raise your hand during the portion at the end of the day set aside for general public comment.

Finally, you may also send your comments via physical mail or email them to regulations@cppa.ca.gov by Friday, May 6th at 6:00 p.m. Note that California law requires that the CPPA refrain from using its prestige to -- or influence to endorse or recommend any specific product or service. Consequently during your presentation, we ask that you refrain from recommending or endorsing any specific product or service.

I now ask the stakeholders who have been assigned to this topic be ready to present. Please use the raise your hand function in Zoom when your name is called so that our moderator can see you. As noted, the moderator will call you in alphabetical order by last name. We will now move to hear comments on the topic of consumer experience with CCPA rights.

Ms. Hurtado, could you please call the first speaker?

MS. HURTADO: Yes. Good afternoon. Our first speaker for this session is Julia Angwin. Julia Angwin, please raise your hand. Thank you. Ms. Angwin, your time starts now. You have seven minutes.

MS. ANGWIN: Thank you so much. Do I have the ability to screen share? Yes. Okay. You can see my slides?

MS. HURTADO: Yes.

MS. ANGWIN: Okay. Great. So I'm a journalist, a longtime technology journalist and the founder of a nonprofit news website called The Markup that covers the impact of technology on society, and have spent a lot of my time writing about the issues of privacy, and so I wanted to share with the panel basically my experiences just briefly about what consumers have experienced in the past and in the present.

So I'm going to start with my first big investigation into privacy was in 2010, and at that time, people did not know that they were being tracked by cookies. So just at that time, you know, we did a big investigation on cookie tracking, and people were really shocked about that. We showed about how people were getting different types of credit card offers that really

discriminated based on where they lived and where -- what kind of income they were predicted to have just based on information that was transmitted when they visited the Capital One website.

And we also showed things like how companies were basically -- knew in advance what you were looking for and could give you different offers, and so these are all things that I think consumers were really surprised about and didn't know was happening.

I then wrote a book in 2014 about how privacy was -- all this information was being collected about everyone, and really the -- what I tried to do in this book was talk about all the ways I tried to protect myself and showing that they were really ineffective and that we needed laws in order to build a baseline privacy standard that everyone could rely on instead of just trying to take their own personal measures.

Of course, the Privacy Act of 2018 was a landmark in that in bringing finally a baseline privacy law to consumers, and obviously has given a lot of access rights to consumers who haven't had them before, and it's certainly been a boon for journalists who have used these rights to try to request information from the -- on themselves or have others request them to write about the. But I do want to say that it hasn't really

prevented some of the more egregious practices that are out there.

So at the news room that I run, The Markup, you know, we have been writing a lot about the phone location data market and how there are dozens of companies who are data brokers who collect the information about people's movements that is sold by the apps on their phone and that -- how there's very little knowledge and oversight about this type of information.

And we have identified, you know, things that are disturbing, like a family safety app, Life360, that was collecting information about everyone. It had, I think more than 30 million users, and people use it to keep track of their kids, but I'm going to assume most of these people, unless they read the fine print, that data was being sold to data brokers, including data brokers who were selling to the government.

After our story, several months later the company said it would stop selling precise location data and instead sell aggregated location data, but as -- as I'm sure, you know, the commission has heard, there are ways to reidentify that type of data, and so it's not always clear that that is enough of a protection.

We've also written about how there's all sorts of date -- services with really, you know, sensitive

information, so dating apps, Muslim prayer apps who are also selling data to data brokers that then sold to the government. And so I bring these up to mention that there is just a certain level of baseline privacy that although in theory people can go in and try to opt out from these things, you know, under the CCPA, there is -- it hasn't prevented this robust market from growing up and trading very sensitive data.

I also just thought it would be fun to share with you a tool that we built at The Markup called Blacklight that lets you see what kind of trackers are --

MR. SOUBLET: If I can interrupt for -- for a moment. You know, as I mentioned in my introductory comments that -- that we can't use the -- the agency's prestige or influence to endorse or recommend a specific product. So we ask that you also not do the same. So can we just skip this part of your presentation?

MS. ANGWIN: Oh. I'm not trying to sell a product. I'm actually just showing you how many trackers are on the CCPA website. So you guys have just one tracker, which is Google Analytics using a remarketing capability that allows visitors to cppa.ca.gov to be tracked on other sites when they leave, and so I just wanted to share with you that in case you didn't know that tracker was on your website.

And I just want to say that, you know, you probably have already seen this article, but Consumer Reports did a study about how easy it is to opt out from CCPA and you know, obviously found that it wasn't as easy as it could be. And so I just wanted to leave you with a thought that leaving these things in the hands of consumers to do the work of opting out is always really difficult and that sometimes, you know, it isn't the full solution. And so that is all. Thank you very much.

MR. SOUBLET: If you can do us a favor, since you submitted -- you have the slides that are on the presentation, we'd like that, to keep it for the record. So can you send them to us at the email address regulations@cppa.ca.gov? We'd appreciate it. Thank you.

MS. ANGWIN: Yes. Absolutely I will send them. Thank you.

MS. HURTADO: Thank you very much for your comment, Ms. Angwin.

Our next commenter is Ginny Fahs. Ginny Fahs, please raise your hand.

We'll move on to the next commenter. Susan Grant. Susan Grant. One moment, please. Okay, Ms. Grant. Your time starts now. You have seven minutes. You may use your camera if you wish. You're muted.

MR. SOUBLET: You're muted.

MS. GRANT: Okay. Thank you. I'm Susan Grant, a senior fellow at Consumer Federation of America. Last year, we partnered with California-based Consumer Action on a project funded by the Rose Foundation to educate Californians about their CCPA rights and encourage them to exercise them.

Last October, we commissioned an online survey in English and Spanish to gauge Californians' awareness of an experience with certain key rights under the CCPA to see their data, to delete their data, and to ask companies not to sell their data. 1,507 adults participated. 69 percent of those surveyed said they'd seen the notice about their privacy rights required by the CCPA on companies' websites they'd visited in the previous twelve months, and many had exercised at least some of their rights, but of those who didn't, the top reason was that they didn't realize they could.

For instance, 47 -- 46 percent had asked at least one business whose website they visited to show them the specific pieces of personal information it collected about them, but of those who never asked, nearly half, 48 percent, gave not knowing they could as the reason why they didn't. Similarly, 47 percent asked at least one business whose website they visited to delete their data, but of those who never made such a request, 51 percent

said they didn't realize they could.

Far more Californians, 63 percent, asked businesses whose website they visited not to sell their data. This may be due to the prominent do not sell my personal information option that businesses that sell such data must display on their home pages. Of those who did not make this request, 42 percent gave not knowing they could as the reason why.

Generally, more younger Californians, and those who identified as black or Hispanics, said they didn't exercise these CCPA rights because they didn't know they could than those were who older and white. More survey respondents at the lower end of the income and educational scales also gave that reason for not making these requests.

There were other answers for which survey respondents could choose to explain why they didn't exercise these rights. One was, I tried and it was too complicated, another was, I didn't think it was necessary, or they could choose none of these reasons. Only about 10 percent of survey respondents who didn't exercise these CCPA rights said, I tried and it was too complicated.

Of those who chose I didn't think it was necessary, fewer were black or Hispanic than white. For instance,

only 24 percent of Hispanics and 30 percent of blacks gave that reason for why they never asked a company whose website they visited not to sell their data compared to 45 percent of whites.

We were surprised by the number of survey respondents who chose none of these reasons for why they didn't exercise these rights; 11 percent of those who never asked a company to show them their data, 13 percent of those who never asked a company to delete their data, and 16 percent of those who never asked a company not to sell their data. What was the reason then that they didn't assert these rights? Unfortunately, we don't know.

We also asked how satisfied those who made the -- these requests were with the businesses' responses. Of those who asked to see or delete their data, 73 percent were very or somewhat satisfied, 71 percent were very or somewhat satisfied with businesses' responses to their request not to sell their data. That means, however, that more than a quarter were not too satisfied or not satisfied at all with the businesses' responses.

We know from Consumer Reports' research that it can sometimes be difficult to make these requests. It's also possible that some Californians aren't sure exactly what to expect when they do.

Finally, we asked if Californians thought businesses should be required to get the permission to collect, use, or share their personal information for any purpose other than to provide the product or service they requested. Nine out of ten said yes.

So what are the main takeaways for your agency from these survey results? First, more research is obviously needed to understand why some Californians aren't exercising their rights and why they're not satisfied with businesses' responses when they do. But even from the results of our brief survey, it's clear that making Californians' actionable rights prominent and easy to exercise is helpful to them.

For instance, the do not sell my personal information option should always be required to be displayed on companies' home pages if they sell such data, and when the CPRA takes effect, the option for not sharing such data should be as conspicuous and easy for individuals to exercise.

The rules to implement the CPRA should be designed to ensure that it's as easy as possible for Californians to be aware of all of their options and to act on them. The survey also shows the need for concerted educational outreach efforts, especially the young people and minority communities.

So my organization, Consumer Federation of America, and Consumers Action have created a guide for Californians about their rights, which will be updated when the CPRA takes effect. It's currently available in English and Spanish as well as Chinese. All the project materials, including the guide, survey results, charts, and press releases are collected at the California Privacy Initiative hub on Consumer Action's website and are also on CFA's website.

Your agency and other stakeholders are welcome to use them. Next week we will hold a webinar for community-based organizations and others who can help educate Californians about their privacy rights and how to exercise them. I'll follow up this meeting by submit -- submitting --

MS. HURTADO: Thirty seconds.

MS. GRANT: -- a written version of my remarks, but thank you very much for your kind attention.

MS. HURTADO: Thank you so much for your comment.

Our next commenter will be Nader Henein. Nader Henein, kindly raise your hand.

Okay. We'll move on to the next one. The next commenter will be Don Marti. Thank you, Mr. Marti. Okay. Mr. Marti, you have seven minutes. Your time begins now.

MR. MARTI: All right. Thank you very much. As a California resident, I have had a right to know how my personal information is used since January 1, 2020, on paper that is. In practice, it turns out to be a little trickier. In order to exercise my California privacy rights, I have had to run a lot of mazes. I won't mention any specific companies here, but I have taken selfies. I have taken a selfie holding my California driver's license. I have scanned my California driver's license front and back. I have taken a photo of my California driver's license from an Android device, had it rejected, found an Apple device, taken a different photo of the same license, and had it accepted.

I have passed a quiz about my former addresses and bank accounts. I have passed a quiz, but only by getting some of the answers wrong because they would have been right if a family member of mine with a similar name was taking the quiz. I have printed and signed a document and scanned it. I have printed and signed a two-page document, gone to a notary public, had it notarized, and scanned it.

So getting through the right-to-know process can be really tricky, and I'm pretty good at paperwork. I have a bunch of different electronic devices I can try. I have a printer, I have a scanner all set up and working

with the right device drivers and -- and all that stuff.

The reason I'm making such a big deal out of getting through my right to know is because right to know is the CCPA right that helped me decide what to do with all my other rights. If I get a positive, sound response to a right to know, then I know I don't have to do a right to delete for that company and I can be more confident in sharing information with them.

There are tens of thousands of companies out there that might have some info on me, so I need to prioritize. Right to know is how I do that, but today, inconsistent and overcomplicated handling of right to know by not just the companies I buy from, but by the data brokers that they use, means that it's really a time-consuming effort for me to find out what's even going on with my personal information.

Under CCPA, I do have the right to use an authorized agent to handle some of this paperwork and complexity for me, but I found that authorized agent requests can be even more complicated. Businesses often get a completely documented authorized agent right to know, and then they turn around and get back in touch with me and make me run through the original maze anyway. And the worst part about all this maze running is sometimes there's no cheese at the end. I've gone all the way through a right

to know with one company, found out, among other things, that they sent my info to some other company, and then I send a right to know to the second company, and they claim they don't have any info on me.

In the case of one high profile company, I can look up the public documents from an ongoing lawsuit, read employee depositions saying that they have certain kinds of information, but then that same company doesn't even share that information with me as required under CCPA. A business should not be able to testify to one thing in court and then turn around and tell California residents something else.

In the 2020 election, Proposition 24 was supported by an overwhelming majority of California voters. Today, the CPPA has an opportunity to implement the intent of those California voters by adopting regulations that make it practical, not just theoretically possible, but actually practical for everyone in California to exercise their basic privacy rights starting with right to know.

As a California resident, I should be able to use a single, simple, standardized right-to-know process, such as requesting a paper form and a business reply envelope, that could be a workable baseline. Naturally, businesses and service providers would compete to offer a variety of different online processes that might be faster and

simpler, but without a guarantee of a common baseline, simple opt-out process, we're still going to be stuck in a maze trying to exercise our privacy rights next year. Thank you very much.

MS. HURTADO: Thank you for your comment, Mr. Marti.

Our next commenter will be Shoeb Mohammed. Please raise your hand. Thank you. Give me just one moment. Okay. Your time starts now. Feel free to use your camera, if you wish, and you have seven minutes.

MR. MOHAMMED: Hello, and thank you for the opportunity to be heard today. My name is Shoeb Mohammed. I'm a privacy and security attorney in the state of California and a member of the board of directors of Meraj Academy Islamic School in Los Angeles, California. I'm also an alumni of that school. And our message today is about our community's experience exercising CCPA rights, and my takeaway is simple. We do not want to allow businesses or any entities for that matter to try to use technicalities to subvert substantive policy and law.

Let me tell you why this is important to us. Meraj Academy is a nonprofit Islamic school that since its founding over thirty years ago, has graduated over three generations of alumni from among the over 500,000 Muslim Americans in LA County.

Our small, but firmly united community represents people from all walks of life, including business owners and entrepreneurs, employees, engineers, refugees, and billionaires. And due to the very real harms that my fellow Muslims know and confront daily, it's important to understand that consumer privacy means a lot more to us than the ability to sell ads or the cost of hiring a consultant.

For us, privacy is the fundamental threshold for keeping our children and our families safe and secure, not just from the threat of government abuse or bad actors, but from businesses and agendas that may have the resources to weaponize technicalities in order to subvert substantive law and policy.

For us, privacy means being free from censor -- censorship and discrimination. It means earning equal opportunities in a world where our own AB testing and anecdotal evidence shows that having the name Mohammed on your resume reduces your algorithmically determined interview requests by over 50 percent, and attempting to post the word Palestine on social media increases the chances that your favorite app will crash, or worse, that your account will be deactivated.

I come from a generation of Muslims who were raised in a post-9/11 America. For our community, privacy is

more than just a right to be profile -- to not to be profiled by an ad company. It's a shield that protects us from systemic persecution. In our community's experience with CCPA rights, we see businesses using technicalities to subvert substantive law, and it demonstrates that attempts to exercise privacy rights are routinely met with technical resistance, a lack of accountability, and we really have no regulatory or legal resource. Like Don Marti just stated in his remarks, we really have no choice but to take their word for it.

Does the auto play algorithm know I'm a Muslim, and how does it use that information to promote content to me or suppress content that I post? And how do I know whether this is by design or by accident? The truth is that no CCPA request can reveal these biases to me. No CCPA request is adequate enough to protect us from systemic harm, or at the very least, allow us to see transparently what the biases are before we are subject to such a system, but they should be, and we should be able to see these biases, even if we cannot stop them.

So with these consumer experiences considering the CCPA rights, from our position, they have been inconsistent, unregulated, and sort of frustrating. We understand the position that businesses are in. Many business owners and technical engineers in these

businesses are members of our community, but we believe that the underlying policies of privacy and the reasons for which people need privacy trump any argument that may try to -- that may essentially in essence try to undermine the -- the very policies and reasons for which we have these privacy statute to begin with.

So with that, I appreciate the time that you have given me to speak today, and I'll -- I'll stop there. Thank you.

MS. HURTADO: Thank you very much, Mr. Mohammed, for your comment.

Our next commenter is Paul Ohm. Paul Ohm. One moment. Paul Ohm. Mr. Ohm, you have seven minutes. Your time starts now.

MR. OHM: Thank you. Good afternoon. I'm a law professor at the Georgetown University Law Center in Washington, D.C. I'm also currently employed by Attorney General Phil Weiser of the State of Colorado. I'm a small part of a team of attorneys assigned by Attorney General Weiser to help implement the Colorado Privacy Act, and I'm here to speak about the Colorado Privacy Act and the inspiration it draws, and the lately just following of the -- the two important privacy laws in California. I'm speaking in my personal capacity, and when I say it doesn't not necessarily represent the views

of Attorney General Weiser or the Colorado Department of Law.

I wanted to take my few minutes to update the agency and the people of California on a very similar undertaking to the one that California is engaging in in Colorado. Like California, the State of Colorado has a comprehensive data privacy law. Our law, which we call the Colorado Privacy Act, or CPA, was signed into law by Governor Polis on July 7th, 2021. It was a result of a bipartisan and overwhelming effort by state legislators. We are the third or were the third state in the country to adopt a comprehensive privacy law.

And one reason why I think it makes good sense to speak about this law on a panel entitled The Consumer Experience with CCP Rights was because our CPA was enacted after both the CCPA and the CPRA had been enacted. Our legislators and state officials expressly mentioned the California laws in their deliberations, and indeed part of the legacy of what the lawmakers and people of California have done with these two laws is the beneficial affect it will have on consumers outside of California through laws like the CPA.

For those who haven't encountered the CPA, it is similar, but has some differences to the laws in California. It sets a set of broad rights for consumers.

It in turn places obligations on some data controllers who conduct business in Colorado or have products or services intentionally targeted to residents of Colorado. It also imposes some obligations on data processors.

And like California, our law makes plain that consumers deserve a right to access, to control the use of their data, to know what information companies collect about them, how that information will be used to enable them to opt out of the sale of their private data by third parties, and other important substantive rights. Like your CPRA, our law explicitly focuses on "dark patterns," which can subvert or impair user autonomy, decision making, or choice.

We too are preparing for a rule-making. The CPA gives the Colorado attorney general's office the authority to promulgate rules for the purpose of carrying out the act. In our current phase, like our counterparts in California, we welcome informal input from all members of the public about any aspect of our upcoming rulemaking, and this fall, we hope to begin a formal notice and comment phase after a notice of rulemaking.

But to give a preview to the public last month, our office issued a document entitled to Pre-Rulemaking Considerations for the Colorado Privacy Act. We wanted to use a document to amplify our call for public in --

input. We wanted to post topics and questions about which we welcome specific feedback, and perhaps a particular interest to those in the California policy-making effort and the California people in general, this memo has a discussion entitled Protecting Coloradans in a National and Global Economy. And in it, we underscore that although or highest priority is of course to protect the people of Colorado, we are mindful that Coloradans, like Californians, participate in national and global markets and networks, and we think our legislator -- legislature enacted a law that is very attentive to complex interjurisdictional context.

And so for -- for example, in speaking of this law, the attorney general of our state said, we want to make Colorado's requirements harmonious and interoperable with requirements adopted by other jurisdictions. States should be able to encounter the rules of our jurisdictions and be able to make sense of both the similarities and the differences.

We hope to write rules mindful of parallel efforts affecting businesses and consumers in California, in other states, and abroad, and so we specifically welcome the input of the kind of people who watch live or the recording of sessions like these in California. We invite your opinions about where the CPA overlaps with

laws like the CCPA and CPRA. We would love to hear ways our rules can address these overlaps to avoid consumer confusion and compliance conflicts. And we also welcome opportunities afforded by sessions like this one to interact directly with government officials in California.

Thank you again for the opportunity to come share the Colorado experience with you. We are confident that the people of our two states will enjoy the benefits of these important new data privacy laws. Thank you.

MS. HURTADO: Thank you for your comment, Mr. Ohm.

Our next speaker will be Hue Rhodes. Mr. Rhodes, please raise your hand. Okay. Mr. Rhodes, feel free to use your camera. You have seven minutes. Your time starts now.

MR. RHODES: Thank you for your -- for the opportunity to contribute. My name is Hue Rhodes. I'm the CEO of Friday. We act as an authorized agent, although I am here speaking not on behalf of Friday, but on behalf of the consumers who are trying to exercise their privacy rights.

In 2020, Attorney General Xavier Becerra said to the U.S. Senate, Americans need robust tools to allow them to understand who has their data, what was collected, if it can be deleted, and how can they opt out of downstream

selling, and it is on the issue of the need for tools that I want to speak.

Our focus has been on the registered data brokers, the over 400 registered data brokers on the state attorney general's website, and what we see is that there is a built-in power imbalance between what resources and tools the consumers have versus the businesses that unfortunately undermine, I think the -- the very good work and the spirit behind the CCPA, and I'll -- I'll talk about that imbalance.

First, businesses are free and do use automated systems to manage requests by consumers. Consumers to date have -- have no real easy way to do that. The emails provided on the website are somewhat effective, but our calculations are that a little less than 50 percent of the responses submitted by email do not end up in any kind of fruitful response.

It would take an infinite amount of leisure time by an individual to submit requests to all the registered data brokers, and then deal with all the responses, making exercising your rights kind of a practical impossibility with respect to data brokers. However, data brokers have the technology tools to manage as many inbound requests as they get.

The second issue is that those responses are often

canned and do not actually accommodate the requests specifically. Many companies respond to the right-to-know request with an automatic deletion, which is to say when consumers submit a request only access -- asking for their right to know, they are greeted with automatic responses saying, we have received your right for deletion and have followed accordingly, which basically denies the consumer the right to actually exercise the right to know because of the preemptive deletion.

We've seen this hundreds of times on the deletion side. I should note we have never seen it the other way. We have never seen a request submitted for deletion responded with a right to know. So it does appear as though there is a reluctance to comply with the right to know.

You also see a variety -- so the -- not only the response is automated, but when they come back, they're actually inaccurate. They don't read the submissions. They respond with automatic deletions.

There is also, as other people have said, no real conforming to the actual mandates of the law in the sense that many will require additional steps that are not prescribed or allowed by the law. Some data brokers even deny the legitimacy of digital signatures as a way of

convening authority. It -- it really does seem to be a bit of the wild west, and all that matters quite honestly from our experience, it seems in the data brokers' world is -- is that they respond with something and that that will do the job. There are often multiple opt-in steps, in addition calls out to consumers to verify, to reauthenticate, et cetera, and then when the consumers do that, these -- these lead to dead ends.

I understand that this is a burden for businesses, and I -- I -- this was covered earlier, but -- but I do believe that there needs to be more facility for consumers to leverage technology for their own advocacy to match the technology used to make these more difficult. I would congratulate California on the -- on the -- the creation of the already authorized agent.

Mr. Ohm from -- from Colorado, if you're listening, I would say that this authorized agent role is extremely important. I do not believe it's in the Colorado law, but is -- is a necessary addition.

Consumers really do need advocates and agents to act on their behalf because the amount of time it would take for them to exercise their rights is just -- makes it virtually impossible and -- and there are no technology tools on the consumer side to match what appear to be the obfuscating tools used on the business side. Thank you

for your time.

MS. HURTADO: Thank you for your comment, Mr. Rhodes.

Our next commenter will be Dusty Roads. Okay. Your time starts now. You have seven minutes. Feel free to use the camera if you wish.

MR. SOUBLET: You're on mute.

MS. ROADS: Sorry. Can you hear me now?

MS. HURTADO: Yes.

MR. SOUBLET: Yes, we can.

MS. HURTADO: Thank you.

MS. ROADS: Okay. I was testing it, and it looked like it was coming out. Okay. Thank you. Good afternoon, everybody. Thank you to the committee and team members for giving me this opportunity to share the consumer experience with the CCPA.

I am Dusty Roads, a privacy protection evangelist and advocate. My comments are specific to the consumer experience with the CCPA. Due to time limits, I will focus my consumer experience remarks on two provisions of the CCPA law, Regulation 1798.50, a private -- a private right to action and Regulation 1798.125, right to nondiscrimination.

I begin my remarks with one -- a one-line quote that sums up the entirety of the consumer experience to date

with the current CCPA law and guidelines, and I quote Viadi Rama (ph.), "What is the purpose of laws if they are unenforceable?" A private right to action is useless if it is unenforceable due to the lack of legal efficacy.

For example, recently, the Supreme Court ruled that in order for the plaintiff to allege an injury, that they must prove concrete, particularized, actual, imminent, and nonconjectorial and hypothetical injury. There is great disagreement across the court -- across the nation by many district courts from the Third District to Ninth of injury and fact and what that constitutes and what is the threshold for the plaintiffs, what they must achieve in order to sue in a particular court or enforce their private right to action under the regulation.

So I would ask the agency in this instance to reexamine the rules on the private right to action and make it actionable for the consumer because as it stands right now, there is no ability for the law to be actionable, to enforce or support or pursue an entity that is blatant and disregards the CCPA regulations.

Further, I would ask the agency in regards to this to also raise the incident minimum from -- from 100 dollars to 30,000 per incident with no cap to ensure entities take consumer data privacy seriously, because unlike some of our presenters today on business

experience, it has not been my experience or experience of many others that I've supported and advocated for that businesses are serious and businesses are interested and diligent about applying the CCPA laws and -- and regulations.

In addition, on -- in respect to the nondiscrimination portion of -- of the regulation and our right for nondiscrimination, many entities are actually discriminating, and no one is enforcing or allowing any remedy for the consumer to address or get -- redress a remedy with the court based on these discrimination acts.

For example, if you go -- all of you can go to your personal health record portal and read the terms of service beyond privacy policy, and you will find out that the vendor that is servicing the portal will tell you straight up very explicitly in big, bold print that they are not subject to HIPPA, that they are going to use your information, and if you disre -- if you do not consent to their use of the information, do not use their portal; do not use the patient portal to get your records, to make appointments. You can do none of it if you don't agree to their -- their privacy policy that provides implicit consent for them to use your data with others, for others, business affiliates, all of them for which are unnamed.

The CCPA only requires companies to provide categories of information. Categories of information is nonactionable for the consumer. A category of information isn't going to tell me how to tell that particular vendor to not use my data, to not sell it, to not provide it to others because I don't have a contact for that vendor because all the CCPA is requiring is categories of information.

I would urge the agency to correct that immediately; that -- to -- to include not only the categories of information, but include the vendors, the names, and the contacts so that we can go and ask and exercise our right with those vendors, because the waivers for the primary provider or data controller prevents us from being able to do that, and they do not take liability or responsibility for their own vendors misusing the data.

I am almost out of time, so I have a lot more to share with you about the ineffectual regulations in the CCPA from a consumer perspective, but I would like to sum it up and simply say please correct the rules so that there is an ability for the consumer to take action. For right now, it's inactionable. Thank you for your time.

MS. HURTADO: Thank you for your comment, Ms. Roads.

Our next speaker and last speaker for this session will be Yadi. Yadi, please raise your hand. Thank you.

Okay, Yadi, your time starts now. You have seven minutes. Feel free to use the camera if you wish.

YADI: Hi. Thank you to the members of the California Privacy Protection Agency for your work and giving consumers an opportunity to talk about experiences attempting to exercise rights under CCPA.

To begin, I was a volunteer researcher for a Consumer Reports study conducted in 2020 verifying the ability for consumers to effectively exercise their privacy rights under CCPA. I submitted do not sell and opt-out requests to several data brokers. Some companies didn't even have opt-out links on their sites. Oftentimes, the process was cumbersome, time consuming, and there were instances where I was just asked -- I was asked to provide even more sensitive data in order to process my request.

Not singling out data brokers, I will share a sampling of my experiences with other companies. Social media platform Facebook has set up what seems to be an efficient, self-service systems for downloading or deleting your data, yet I couldn't access or delete my data. This is because although Facebook had no problem with me being just Yadi with a butterfly profile picture for ten years, as soon as I started posting about privacy on the platform, Facebook locked my account and

instructed me to confirm my identity with a government-issued ID.

So in order to access my data, I had to do it within my Facebook account, and in order to access my account, I had to submit more personal information to Facebook. My emails to Facebook have been acknowledged with automated responses. This example may seem like an outlier, but I should still be able to access and delete my data without giving up extra personal information or being required to have an account. I didn't trust Facebook with my data then, and I definitely don't today.

Other social media companies hoover your data from friends on their platforms, for example, importing or sharing access to your contacts on platforms like LinkedIn and Clubhouse. And I shouldn't have to create accounts on various social media platforms just to submit a request to have my data deleted.

Wireless provider T-Mobile has yet to acknowledge my do not sell request email. T-Mobile directs consumers to download a separate app to exercise their rights. I did not get a notification from them about their massive data breach, which has led to a flood of spam texts ever since.

Fast food chain McDonald's has their employees ask consumers to download the McD's app before taking your

order. If you attempt to download the app, the first thing it does is force you to turn on location sharing. If you don't accept, you can't use the app. No financial incentive notice, no opt-out, nothing.

Online marketplace thredUP is a gem of maddening dark patterns like running sales that require you to check out within one hour of adding an item to your shopping cart. Talk about creating massive FOMO. The only way to opt out is to not shop during those hours or days that these promos are running. Imagine having that experience at a physical brick-and-mortar store.

Data analytics Vigilant Solutions provides license plate reader equipment to law enforcement agencies. They responded to my CCPA request by stating it had no information on file for me, but I was able to get the information that they did in fact have on me through a public record request I submitted to my local police department.

Automotive company Tesla, of the various issues, I want to draw attention to their use of facial recognition whereby they slip in a request for a selfie when finalizing your purchase and delivery transaction online. No explanation or notice, but if you leave the browser or go back, poof, it magically disappears and you can just proceed to finalize paperwork electronically, no selfie

needed. I was not the owner of this vehicle, just doing the paperwork on the owner's behalf. So would Tesla have voided the entire transaction and purchase if I had uploaded my picture?

Google privacy controls are still weak for U.S. consumers. The online browser Chrome has yet to implement global privacy control or provide other meaningful opt-outs like it's been rolling out for EU consumers.

Because of the recent headlines about the Supreme Court's potential ruling to reverse a woman's right to choose, my last example will be of fertility tracking apps. Flo, where millions of women have shared their personal health data, assured users like myself that our data was kept private when in fact Flo was sharing our sensitive information with third parties like Google and Facebook.

You are probably aware of the FTC settlement with Flo in 2021 for its deliberate, rampant, and persistent privacy violations, including allegations that Flo had in fact lied to its users about sharing sensitive data with third parties.

Furthermore, Flo is not the only woman's health tracking app to abuse consumers' privacy and security. In 2020, GLOW was fined by the California State Attorney

General, and competitors Clue and My Days were also ousted for privacy leaks. Privacy and trust is vital. Who knows what other entities could take advantage of sensitive data like periods, pregnancies, miscarriage, abortions, and sexual practices and use that information to further discriminate against women or face criminal prosecution.

To conclude, data minimization is essentially -- is essential, especially in the light of an ever-growing number of data breaches and the additional negative externalities, both present and future. I ask the agency not to dilute privacy requirements for the sake of aligning with other privacy laws or easing the burden on companies. Protecting privacy and data is a cost of doing business in modern times, like paying for internet. CCPA has the opportunity to develop protections that are nuanced to Californians and can fill gaps of other privacy laws in the US. Privacy is autonomy. Thank you.

MS. HURTADO: Thank you, Ms. Yadi for your comment.

MR. SOUBLET: That was our last speaker for this session. We want to thank everyone who spoke during our sessions today. We now have time to move into our -- our general public comment session.

Speakers who wish to speak should raise their hand using the raise your hand function, which can be found in

the reaction feature on the bottom of your Zoom screen. You will be called in the order that they -- they appear. When it is your turn, the moderator will invite you to unmute yourself, and then you will have -- unlike the other session, you will have only three minutes to provide your comments. We want to accommodate as many people as possible.

We will be strictly keeping time. When your comment is completed, the moderator will mute you. Please note that your name may be visible to the public during this live session and our subsequent recording. If you prefer, you may also send us your comments via physical mail, or you can email them to regulations@cppa.ca.gov by 6 p.m. this Friday, May 6th.

With that, I'll turn it over to -- I'll note that California law requires the CPPA to refrain from using its prestige or influence to endorse or recommend any specific product or service, so during your comments, we ask that you also refrain from recommending or endorsing any specific product or service. During this -- a reminder is that during this general public comment period, please raise your hand if you would like to speak.

Ms. Hurtado, could you please call the first speaker?

MS. HURTADO: The first speaker is Edwin Lombard. Okay. Mr. Lombard, your time starts now. You have three minutes. Feel free --

MR. LOMBARD: Okay.

MS. HURTADO: -- to use the camera if you wish.

MR. LOMBARD: Yes. My name is Edwin Lombard. I'm calling as a concerned small business owner about the lack of transparency related to the stakeholder process and these meetings. Three days of Zoom meetings does not replace the need -- the need to get substantive input and real -- from real people on the ground. Additionally, we haven't even seen draft concepts of what we are supposed to be commenting on today.

These stakeholder sessions appear to be front-loaded before thoughtful input could be incorporated just to check a box. I understand the need to protect California's privacy, but it's also critical to protect small businesses from the damages -- damaging effects and regulations that have been rushed and have not included our input. Real people do not have time to tune in to three-day meetings and keep track of the rapidly changing real -- rulemaking process that has yet to involve them in a meaningful way. They have jobs, they have customers to serve, employees to look after, and communities to build.

The CPPA continues to hurdle towards missing the statutory deadline that is the final regulations within a formal legal extension, which sends the wrong message to Californians about legal compliance. I have been working with other black-owned small businesses in my community to help them to prepare for the -- the regulations, but that's a near impossible task without draft regulations.

To make it worse, the CPPA has made no substantial outreach to our communities. What is CPPA doing to address the concern of small business owners? Previous comments of CPPA that these regulations will not impact small business are simply not true. For example, the required an -- analysis of economic impact to business has not been prepared or provided. To put a finger -- a finer point on it, the CPPA has yet to show how many black-owned businesses will be created or forced to close by this regulation.

It is important that you not ignore or overlook the economic impact requirements. CPPA must show these numbers to our community and allow us to give thoughtful feedback before any regulations are adopted in order to minimize impact on small businesses --

MS. HURTADO: Thirty seconds.

MR. LOMBARD: -- as these regulations shape. Small businesses like mine have been through so much in the

pandemic. It must be considered as we -- as you go forward with the rulemaking process. Thank you.

MS. HURTADO: Thank you, Mr. Lombard, for your comment.

Our next commenter is going to be Thomas Gerhart.

Okay. Mr. Gerhart, you have three minutes. Your time starts now.

MR. GERHART: Hi. Thank you for the opportunity to speak for this rulemaking. I'm just going to share a couple of areas that I've noticed personally. I am a former law student, now practicing attorney speaking to you just as a concerned citizen. While I was a law student, I tracked and was published regarding the 2018 statute that was enacted as well as Proposition 24.

During that time, I marked my calendar for when the 2018 legislation went live in January of 2020, and I had a list of businesses that I was going to call and request that they delete my data. I am pleased to report that many of the businesses did comply with that. However, I found two areas that regulations should probably address in the future.

The first is I had contacted a telecommunications company to request that they delete my data. They said unfortunately they could not, but their practice was to take my Social Security number from my account and move

that information into the account number field so they could always pull my -- my account up by using my Social even when I was no longer a customer of theirs. In that, that kind of created this awkward if there's a data breach in the future, somebody would still get my name and my Social even though the business did not brand it as a Social.

And the second example of a little bit of a failing with this is something that some of the other people have called in about where there are too many hurdles necessarily to submit these requests. It's not a very non -- just, you know, Joe the plumber system where, you know, somebody who isn't very tech savvy can jump in and submit their request, and in some instances, the focus is a little bit too much on precision and less on authentication.

For example, I submitted a data request to a hospitality company, and they said that they couldn't find my information, and what it boiled down to is I had been giving them my first and last name per their request, Thomas Gerhart, but for whatever reason, they had my middle initial in the system, and it -- they kept rejecting it, and then it triggered that one-year period where they didn't have to respond anymore.

Ultimately I learned that once I told them it was

Thomas M. Gerhart --

MS. HURTADO: Thirty seconds.

MR. GERHART: -- they processed the request accordingly. So I -- I think, you know, if you have ninety-nine percent accuracy on the data that you're reporting and there's just one thing that's just not lining up, perhaps there can be a little bit more leeway in the regulations for permitting the deletion of information. Thank you for your time. Good luck with the rulemaking. I appreciate everything you guys do. Thank you.

MS. HURTADO: Thank you so much for your comment.

Our next commenter will be Ginny Fahs. Okay. Okay. Ms. Fahs, your time starts now. You have three minutes. Feel free to use your camera if you wish.

MS. FAHS: Hello there. My name is Ginny Fahs, and I work at Consumer Reports. My group at Consumer Reports has conducted three research studies on CCPA data rights with over 800 consumers. Consumers say it is difficult to use their rights. They say that they don't understand how much work they would have to do. One consumer said they were angry that companies were flouting the law. And finally a consumer said that it was complicated, there were a lot of links, and it just was -- it just wasn't clear to them what to do.

At a high level, consumers are having a hard time with three things. They're having a hard time with discovery of companies that may have their data, with initiating the request to those companies, as well as with identity verification. And while authorized agents are not a silver bullet for these problems, they can help with all three of them. Consumers have said this is a tedious, repetitive process that I'd much rather delegate to a competent agent, and another consumer said that an agent service would be really nice to use if only it could work well.

Agents are facing a lot of barriers when they try to do the work of submitting requests for consumers. Those business -- those barriers are that, one, businesses sometimes just are not prepared to accommodate agents. They'll have fields on their forms that say things like first name or what's the maiden name of the agent when often the agent is an organization.

The agent processes and flows are inconsistent. Sometimes a company will send data requested by an agent to the agent rather than the consumer, and sometimes they'll send it to the consumer, but not the agent, and the consumer doesn't get to specify. There's also lack of communication with authorized agents, and agents are often out of the loop as to the status of requests.

Finally, power of attorney that agents receive can be ineffective with companies, and companies will ask for further identification even where there is a power of attorney on file. So because of that, we have a few recommendations. First, we think that the regulation should make sure consumers are allowed to specify who receives the data they access when they use their CCPA rights, the consumer or the agent.

Finally, we encourage an exploration of expanding the power of attorney authorization to include digital methods and solutions. And finally, we would ask that regulators consider permitting the use of a standard protocol --

MS. HURTADO: Thirty seconds.

MS. FAHS: -- to send and receive requests.

So with the right adjustments from regulators, we believe that the consumer experience of CCPA will continue to improve. Thank you for your time.

MS. HURTADO: Thank you very much for your comment, Ms. Fahs.

Our next commenter is Elizabeth. Elizabeth, you have three minutes. Your time starts now. Feel free to use your camera if you wish.

MS. GRAHAM: Thank you so much. My name is Elizabeth Graham. I'm currently the executive director

for the California Fuels & Convenience Alliance. A little bit about the organization I've worked for, we represent the gas station small business owners. There's about 9,000 gas stations in the Cal -- in California.

CFCA is a lifeline of our economy offering California consumers and businesses transportation, fuel, and energy from manufacturers to the end customers. This includes wholesale or retail participants, who then deliver fuel to the individual users, such as the gas stations I mentioned, but also including the farmers, government agencies, fleet fueling. And so our members really serve every single region, city, county in this great state.

As a majority of our members are small business owners, many of them being family-owned businesses passed down from one generation to the next, CFCA has significant concerns with potential costly, confusing and uncertainty around new data privacy regulations that this board will be considering. It is our goal to conveniently and safely provide quality fuels, goods, and foods to meet the needs of every family and community in California.

Our concerns around potential data and privacy regulations are that the convenience at which we provide our goods could be negatively impacted. While our

members support the data privacy rights, of course, of their consumers, these regulations cannot be developed and implemented at the expense of jeopardizing small businesses across the state. Many of our members rely on digital tools and services to manage these operations, reach their current potential customers, and promote their business.

With so many recent changes to California's data privacy laws, or members, like many other small businesses, are incredibly confused on how to comply and what does or does not impact them and the law. We have consumer data for ourselves, but many of our members are unclear about the current law, much less knowing what new regulations are being proposed.

CFCA encourages the CPPA board to take a more measured approach with California businesses, one that hinges on collaboration, practicality, and support as opposed to punitive, disruptive, and (indiscernible) --

MS. HURTADO: Thirty seconds.

MS. GRAHAM: Thank you. The State of California has a role to play in protecting the data rights of consumers, but that role should not include imposing overbearing costs. Thank you so much for your time.

MS. HURTADO: Thank you, Ms. Elizabeth, for your comment.

If there are any other commenters, please raise your hand at this time. I see no other hands raised at this time.

MR. SOUBLET: I'd like to thank all of the presenters and commenters today and especially those of you who commented in our just concluding public comment period. A recording of the presentations will be on our website when processed.

Tomorrow, we will start again at 9 a.m. with our second day of sessions for those that have signed up to speak, and then we will at the end of the day tomorrow again hold a public comment session. So if we missed you today, you will have an opportunity to speak again tomorrow.

Again, our session tomorrow, May 5th, will resume at 9 a.m., and we really want to thank everyone for participating in today's sessions. Thank you.

(End of recording)

TRANSCRIBER'S CERTIFICATE

STATE OF CALIFORNIA)

)

COUNTY OF SACRAMENTO)

This is to certify that I transcribed the foregoing pages 1 to 145 to the best of my ability from an audio recording provided to me.

I have subscribed this certificate at Phoenix, Arizona, this 11th day of June, 2022.

_____

Brittany D. Payne

eScribers, LLC