

1                   AMENDED TRANSCRIPTION OF RECORDED STAKEHOLDERS  
2                   SESSION OF CALIFORNIA PRIVACY PROTECTION AGENCY

3  
4                   MAY 4, 2022

5                   VIA TELECONFERENCE

6  
7 Present:           ASHKAN SOLTANI, Executive Director  
8                   BRIAN SOUBLET, Interim General Counsel  
9                   JENNIFER URBAN, Chairperson  
10                  TRINI HURTADO, Conference Services  
11                  Coordinator

12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22 Transcribed by:   Alaina L. Russell,  
23                   eScribers, LLC  
24                   Phoenix, Arizona

25                   --o0o--

1                   **AMENDED TRANSCRIBED RECORDED PUBLIC MEETING**

2                   **OF CALIFORNIA PRIVACY PROTECTION AGENCY**

3                   **May 4, 2022**

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

15           Chairperson Urban?

16           **MS. URBAN:** Thank you Executive Director Soltani.  
17 Good morning, everyone. My name is Jennifer Urban.  
18 I am the chairperson of the board for the agency. I'd  
19 like to thank our executive director and all of the staff  
20 who have been working on this for inviting me today to go  
21 over our pre-rulemaking activities and to invite your  
22 participation over the next few days.

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

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

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

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

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

25 I believe Executive Director Soltani will say more

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

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

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

24 **MR. SOLTANI:** Thank you, Chairperson Urban.

25 Before we get started with the substance of the day, I

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

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

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

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

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

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

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

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

1 estimated.

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

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

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

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

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

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

23 Finally, you may also send us your comments via  
24 physical mail or email to [regulations@coppa.ca.gov](mailto:regulations@coppa.ca.gov) by  
25 Friday, May 6th at 6 p.m. Note, California law requires



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

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

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

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

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

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

4 **MS. ADEY:** Hi, can you hear me?

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

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

13 The Personal Insurance Federation represents seven  
14 of the state's largest home and auto insurers. Our  
15 association deals exclusively in personal, property, and  
16 casualty lines. We believe it's important to understand  
17 that the insurance industry is already a highly regulated  
18 industry in general particularly on issues of privacy.  
19 The state's insurance commissioner heads the largest  
20 consumer protection agency in the United States with over  
21 1,300 staff at a 300-million-dollar budget.

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

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

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

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

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

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

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

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

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

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

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

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

11 Our next commenter will be Meredith Broussard.

12 Meredith, you now have seven minutes.

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

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

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

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

25 We can use computational systems to analyze human

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

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

25 If we assume that automated systems discriminate by

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

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

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

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



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

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

9 Our next commenter will be Hilary Cain.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

10          Our next speaker will be Jarrell Cook.

11          Can you please raise your hand Jarrell Cook?

12 Jarrell Cook? Okay, we'll come back to Jarrell Cook.

13          Our next speaker will be Alyssa Doom.

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

17          **MS. DOOM:** Thank you. Good morning, Chair Urban and  
18 members of the California Privacy Protection Agency.

19 Thank you for this opportunity to provide input on the  
20 upcoming rulemaking under the California Privacy Rights  
21 Act.

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

25          CCIA is a nonprofit, nonpartisan trade association

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

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

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

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

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

1 medical treatment, public assistance, or credit  
2 decisions.

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

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



1 consumers.

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

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

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

1 precautions taken instead of offering opt-out options.

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

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

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

18 Our next --

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

22 **MS. HURTADO:** Thanks, Brian.

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

25 Jarrell Cook, please raise your hand.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

12 Okay. Commenter after that is Cathy O'Neil.

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

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

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

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



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

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

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

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

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

25 In order to distinguish higher risk automated

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

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

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

25       In developing regulations on this topic, we

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

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

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

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

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

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

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

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

25 The Future of Privacy Forum has published many

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

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

6 Our next commenter will be Chris Riley.

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

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

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

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

25 Now, while I understand and sympathize with the

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

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

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

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

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

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



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

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

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

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

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

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

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

21           **MS. HURTADO:** 30 seconds.

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

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

1           Our next commenter will be Ridhi Shetty.

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

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

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

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

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

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

1 particular final outcome related to a person.

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

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

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

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

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

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

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

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



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

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

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

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

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

3           Our next commenter will be Carl Szabo.

4           Carl Szabo, please raise your hand.

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

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

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

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

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

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

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

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

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

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

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

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

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

1 imagine, that we could actualize these rights.

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

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

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

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

3 **MS. HURTADO:** Thirty second warning.

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

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

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

15 Mr. Winters was the last commenter for this session.

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

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

4 (Whereupon, a recess was held)

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

7 (Pause)

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

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



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

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

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

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

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

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

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

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

25       Please plan -- plan to focus your initial comments on

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

6 Finally, you may also send us your comments via  
7 email or mail, and email them to [regulations@coppa.ca.gov](mailto:regulations@coppa.ca.gov)  
8 by Friday, May 6th, at 6 p.m.

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

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

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

25 **MS. HURTADO:** Okay, thank you, Brian.

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

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

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

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

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

9       4A's members are also significant employers in  
10 California, operating more than 198 member offices in the  
11 state. Advertising is a significant contributor to the  
12 U.S. economy. In August 2021, IHS Markit research report  
13 found that in 2020, advertising spend supported 1 -- 7.1  
14 trillion in U.S. output, and 28.5 million U.S. jobs. The  
15 research also determined every dollar of ad spending  
16 supported on average over 21 dollars of economic output.

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

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

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

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

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

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

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

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

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

1 process a single data subject request. The volume of  
2 data subject requests almost -- nearly doubled between  
3 2020 and 2021, with the cost of processing them soaring  
4 to approximately 400,000 per million identities.

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

10 Compliance costs also disproportionately affect small  
11 businesses. Small businesses with fewer than twenty  
12 employees would incur approximately 50,000 in initial  
13 costs, while medium businesses with employees between  
14 twenty and a hundred could incur an additional cost of  
15 100,000 dollars. New data requirements in the CPRA will  
16 almost certainly increase privacy compliance costs from  
17 any agencies in 2023 if the CPRA closes the selling  
18 versus sharing loophole and clarifies that covered  
19 businesses must give California residents the option to  
20 opt out if their data is sold or shared with a third  
21 party for advertising purposes. This suggests that  
22 companies will see a considerable jump in the number of  
23 requests they receive.

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



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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

12 **MS. HURTADO:** Thirty second warning.

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

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

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



1 you're available?

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

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

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

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

1 colleagues, Tracy Shapiro.

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

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

1 possible.

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

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

1 contractors to flow down the required terms to their  
2 subcontractors.

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

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

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

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

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

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

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

1 999.315(c) of the existing CCPR regulations until it can  
2 be replaced with new regulations for an optional opt-out  
3 preferice -- preference signal that is consistent with  
4 the CPRA's requirements.

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

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

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

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

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

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

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

1 data protection regulation, end of quote.

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

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



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

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

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

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

1 for our businesses.

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

10 Thank you so very much for your time.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

25       And -- and any guidance or clarification around

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

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

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

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

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

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

15 **MS. HURTADO:** Time, Mr. Kingman.

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

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

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

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

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

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

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

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



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

4 In a January report by Information Technology and  
5 Innovation Foundation, ITIF, a nonprofit, nonpartisan  
6 research and educational institute, finds that since  
7 2018, thirty-four states have passed or introduced  
8 seventy-two privacy bills, regulating the commercial  
9 collection and use of personal data. Many California  
10 businesses operate outside the state lines, which means  
11 they are subject to a myriad of privacy policies, not to  
12 mention an additional layer of privacy mandates specific  
13 to certain industries, such as the financial sector that  
14 have been in place for years.

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

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

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

20       My thanks to you for receiving our comments this  
21 afternoon.

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

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

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

3 **MR. RECTOR:** Very good. Well thank you for the  
4 opportunity to address you today. My name is Clark  
5 Rector. I'm the executive vice president of government  
6 affairs for the American Advertising Federation. The AAF  
7 is the umbrella association for the advertising industry.  
8 Our corporate membership includes many major advertisers,  
9 advertising agencies, and the media, including print,  
10 broadcast, outdoor, and online media. We also represent  
11 over 35,000 advertising professional -- professionals in  
12 150 local advertising federations across the country,  
13 including ten California advertising associations.

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

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

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

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

12       In 2020, the commercial internet generated more than  
13 17 million U.S. jobs, and it's important to remember that  
14 of those jobs, more of them actually came in small  
15 businesses than in the largest internet companies, and  
16 all of this is made response -- made possible by the  
17 responsible use of data.

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

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

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

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

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

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

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

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

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

21 **MR. WALSH:** Good afternoon.

22 **MS. HURTADO:** Your time starts now.

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

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

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

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

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

4 **MS. HURTADO:** Mr. Walsh.

5 **MR. WALSH:** -- broadly.

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

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

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

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

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



1 of an employer.

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

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

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

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

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

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

11       **MR. WALSH:** I'd be happy to.

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

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

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

25               (Whereupon, a recess was held)

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

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

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

25       We will proceed through the program according to the

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

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

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

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

1 to provide your comments.

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

11 Finally, you may also send your comments via  
12 physical mail or email them to [regulations@coppa.ca.gov](mailto:regulations@coppa.ca.gov) by  
13 Friday, May 6th at 6:00 p.m. Note that California law  
14 requires that the COPPA refrain from using its prestige  
15 to -- or influence to endorse or recommend any specific  
16 product or service. Consequently during your  
17 presentation, we ask that you refrain from recommending  
18 or endorsing any specific product or service.

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

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

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

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

10 **MS. HURTADO:** Yes.

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

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

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

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

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

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

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

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

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

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

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



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

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

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

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

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

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

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

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

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

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

25           **MR. SOUBLET:** You're muted.

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

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

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

1 said they didn't realize they could.

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

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

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

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

1 only 24 percent of Hispanics and 30 percent of blacks  
2 gave that reason for why they never asked a company whose  
3 website they visited not to sell their data compared to  
4 45 percent of whites.

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

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

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

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

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

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

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

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

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

16       **MS. HURTADO:** Thirty seconds.

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

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

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

22       Okay. We'll move on to the next one. The next  
23 commenter will be Don Marti. Thank you, Mr. Marti.

24       Okay. Mr. Marti, you have seven minutes. Your time  
25 begins now.

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

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

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



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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 of Attorney General Weiser or the Colorado Department of  
2 Law.

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

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

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

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

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

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

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



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

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

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

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

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

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

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

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

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

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

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

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

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

25 The second issue is that those responses are often

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

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

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

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

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

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

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

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

1 for your time.

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

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

7 **MR. SOUBLET:** You're on mute.

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

9 **MS. HURTADO:** Yes.

10 **MR. SOUBLET:** Yes, we can.

11 **MS. HURTADO:** Thank you.

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

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

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

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

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

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

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

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

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

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



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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

8 We will be strictly keeping time. When your comment  
9 is completed, the moderator will mute you. Please note  
10 that your name may be visible to the public during this  
11 live session and our subsequent recording. If you  
12 prefer, you may also send us your comments via physical  
13 mail, or you can email them to [regulations@cppa.ca.gov](mailto:regulations@cppa.ca.gov) by  
14 6 p.m. this Friday, May 6th.

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

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

1           **MS. HURTADO:** The first speaker is Edwin Lombard.

2           Okay. Mr. Lombard, your time starts now. You have three  
3           minutes. Feel free --

4           **MR. LOMBARD:** Okay.

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

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

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



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

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

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

23       **MS. HURTADO:** Thirty seconds.

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

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

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

5 Our next commenter is going to be Thomas Gerhart.

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

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

15 During that time, I marked my calendar for when the  
16 2018 legislation went live in January of 2020, and I had  
17 a list of businesses that I was going to call and request  
18 that they delete my data. I am pleased to report that  
19 many of the businesses did comply with that. However, I  
20 found two areas that regulations should probably address  
21 in the future.

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

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

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

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

25 Ultimately I learned that once I told them it was

1 Thomas M. Gerhart --

2 **MS. HURTADO:** Thirty seconds.

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

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

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

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

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

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

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

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

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

14       **MS. HURTADO:** Thirty seconds.

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

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

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

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

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

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

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

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

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

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

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

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

19       **MS. HURTADO:** Thirty seconds.

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

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



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

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

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

15       Again, our session tomorrow, May 5th, will resume at  
16 9 a.m., and we really want to thank everyone for  
17 participating in today's sessions. Thank you.

18       (End of recording)

19  
20  
21  
22  
23  
24       TRANSCRIBER'S CERTIFICATE  
25

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25

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*

\_\_\_\_\_

Brittany D. Payne  
eScribers, LLC