

PUBLIC HEARING  
ON THE CALIFORNIA CONSUMER PRIVACY ACT (CCPA)

February 5, 2019

10:00 a.m.

1500 Capitol Avenue  
Sacramento, California

Mandy M. Medina, CSR No. 11649

APPEARANCES

The Hearing Officer:

STACEY SCHESSER, Supervising Deputy Attorney General,  
State of California, Office of the Attorney General

Also Present:

LISA B. KIM, Deputy Attorney General, State of  
California, Office of the Attorney General

DANIEL BERTONI, Staff Services Analyst, State of  
California, Office of the Attorney General

1 PUBLIC HEARING

2 ON THE CALIFORNIA CONSUMER PRIVACY ACT (CCPA)

3 February 5, 2019 - 10:11 a.m.

4  
5 THE HEARING OFFICER: Good morning. On behalf  
6 of the California Department of Justice and Attorney  
7 General, Xavier Becerra, welcome to the fifth public  
8 forum on the California Consumer Privacy Act.

9 We are at the beginning of our rulemaking  
10 process on the CCPA. These forums are part of an  
11 informal period where we want to hear from you. There  
12 will be future opportunities where members of the public  
13 can continue to be heard, including once we draft a text  
14 of the regulations and enter the formal rulemaking  
15 process.

16 Today, our goal is to listen. We are not able  
17 to answer questions or respond to public comments.

18 Before we begin, we would like to briefly  
19 introduce ourselves. My name is Stacey Schesser. I am  
20 a Supervising Deputy Attorney General for the Privacy  
21 Unit, which is part of the Consumer Law Section.

22 MS. KIM: Hi. Lisa Kim, the Deputy Attorney  
23 General also in the Privacy Unit.

24 MR. BERTONI: I'm Daniel Bertoni and I'm a  
25 researcher in the Attorney General's executive office.

1 THE HEARING OFFICER: We will begin in just a  
2 few moments, but we have a few process points we would  
3 like to cover for today's forum. Each speaker will have  
4 five minutes. Please be respectful of the timekeeper,  
5 which is Daniel, and your fellow speakers here today.  
6 He will let you know when your time is coming to an end  
7 by showing you very handy forms.

8 We also have a court reporter here who is  
9 transcribing comments. Please speak slowly and clearly.

10 The front row is reserved for speakers. When  
11 you come up to the microphone, it is requested, but not  
12 required, that you identify yourself when you are  
13 offering your public comment. It would also be helpful  
14 if you have a business card that you can hand to the  
15 court reporter.

16 We welcome written comments that can be sent  
17 to us by E-mail or mail. We also want to note that we  
18 now have a deadline for when we would like to receive  
19 comments by, and that's March 8th, 2019, after we have  
20 concluded all of our public forums. We have also added  
21 a final public forum at Stanford University on  
22 March 5th, and that will begin at 12:45. There is more  
23 information on our website to learn about the location  
24 of that.

25 The bathrooms are outside and to the left of

1 this room.

2 And then before we begin, I would like to ask  
3 if there are any media present, if you could please  
4 raise your hand. Thank you.

5 So just to briefly go over the background on  
6 the rulemaking process, we are governed by the  
7 California Administrative Procedures Act. During this  
8 process, the proposed regulations and supporting  
9 documents will be reviewed by various state agencies,  
10 including the Department of Finance and the Office of  
11 Administrative Law.

12 Right now, these public forums are part of our  
13 initial preliminary activities. This is the public's  
14 opportunity to address what the regulations should  
15 address and set. We strongly encourage the public to  
16 provide oral and written comments, including any  
17 proposed regulatory language, so that we can take them  
18 into consideration as we draft the regulations.

19 Once this informal period ends, there will be  
20 additional opportunities for the public to comment on  
21 the regulations after a proposed draft is published by  
22 OAL. We anticipate starting the formal review process,  
23 which is initiated by a filing of a Notice of Regulatory  
24 Rulemaking, in early fall of 2019.

25 The public hearings that take place during the

1 formal rulemaking period will be live and webcasted and  
2 videotaped. All written comments and oral comments  
3 received during those public hearings will be available  
4 on-line through our CCPA web page, which is here.

5 We encourage you to stay informed throughout  
6 the process by continuing to visit our website at  
7 [www.oag.ca.gov/privacy/ccpa](http://www.oag.ca.gov/privacy/ccpa).

8 Finally, we are going to walk through some of  
9 the areas on which we will be seeking public comment.  
10 CCPA section 1798.185 of the civil code identifies  
11 specific rulemaking responsibilities of the AG. The  
12 areas are summarized here in 1 through 7. Please keep  
13 in mind these areas when providing your comments today.

14 Should there be -- number 1, should there be  
15 additional categories of personal information?

16 Number 2, should the definition of unique  
17 identifiers be updated?

18 Number 3, what exceptions should be  
19 established to comply with the state or federal law?

20 Number 4, how should a consumer submit a  
21 request to opt out of the sale of personal information,  
22 and how should a business comply with that consumer's  
23 request?

24 Number 5, what type of uniform opt-out logo or  
25 button should be developed to inform consumers about the

1 right to opt out?

2 Number 6, what type of notices and information  
3 should businesses be required to provide, including  
4 those related to financial incentive offerings?

5 Number 7, how can a consumer or their agent  
6 submit a request for information to a business, and how  
7 can the business reasonably verify these requests?

8 At this time, we welcome comments from the  
9 public. Speakers, please come down to the front row.

10 I also want to note that we will be taking a  
11 break at some point during today's forum when there is a  
12 bit of a lull in speakers. We will be taking a natural  
13 break to also give an opportunity for our court reporter  
14 to have a quick break as well.

15 At this time, I invite anyone who is  
16 interested in speaking to please come down to the front  
17 row and come up to the mic. Thank you.

18 MS. ROSA: All set? Good morning, Kris Rosa  
19 on behalf of the Nonprofit Alliance.

20 When the CCPA was being negotiated and drafted  
21 last year, legislators exempted nonprofits from the  
22 bill. We're grateful to legislature for the clear  
23 intent to exclude nonprofits from the direct hit of the  
24 costly impact of this legislation.

25 Nonprofits, however, are still nevertheless

1 impacted, because we do not operate in a vacuum. We use  
2 consumer data and third party providers to ensure our  
3 programmatic and fundraising marketing messaging are  
4 delivered to the most likely to benefit and likewise not  
5 to those who will not.

6 Nonprofits do not have a profit margin to  
7 allow them to blanket the state to every resident who  
8 would, for example, support the Sierra Club.

9 If, though, we use data to connect those in an  
10 appropriate way, if you buy hiking boots at REI, for  
11 example, you may be interested in helping support nature  
12 conservancy efforts. It is more efficient, more  
13 cost-effective, and better for potential donors for  
14 nonprofits to use data in this manner.

15 As an example of how we use data for  
16 programmatic efforts, the ARP is a good example. When  
17 seniors are in crisis and they are removing themselves  
18 further and further from society and they become in  
19 desperate straits and close themselves off. They tend  
20 to not raise their hands to ask for help. ARP has to  
21 seek them out and they have to find them. At ARP, they  
22 use data to see if a senior is, for example, only buying  
23 three food products in a month. They can then go in and  
24 find that senior and connect them to vital services.

25 We also rely on commercial data companies to



1 maintain our data in secure environments at a level that  
2 many nonprofits could not afford to maintain on their  
3 own, and certainly not without reducing the funds that  
4 they would otherwise spend on their direct mission work.

5 The legislative exemptions, therefore, while  
6 wonderfully well-intentioned, can adequately protect us  
7 from the costly impact of the CCPA. In fact, we may be  
8 the first to suffer the full impact of changes when our  
9 commercial partners are forced to give us an ultimatum  
10 due to the increased cost of complying with the CCPA:  
11 Pay us more or cease entirely your outreach to  
12 12 percent of the United States population residing in  
13 California.

14 Interestingly, probably not surprisingly, to  
15 those of us who live in California, Californians are  
16 especially charitable and represent 20 percent of all of  
17 the fundraising support to national organizations  
18 throughout the country. Their proportional value to  
19 smaller state and regional organizations is naturally  
20 even then greater. It's not exaggeration to say that  
21 restricting the ability to reach California donors due  
22 to the cost impacts of CCPA will be devastating to the  
23 U.S. nonprofit sector.

24 There are some concerns with the CCPA, and in  
25 a way that they will negatively impact nonprofits and

1 beneficiaries and the work that we do on their behalf.

2 First, without significantly clarifying the  
3 scope of obligations related to the disclosure of  
4 information to consumers, we are unnecessarily driving  
5 up the cost of data. The CCPA will almost certainly  
6 require significant stat augmentations by most data  
7 providers unless the scope is reduced and/or clarified.

8 A large part of the burden will be handling  
9 requests to consumers with copies of particular pieces  
10 of personal data. Data providers have many different  
11 types of information. Much of it is meaningless to  
12 consumers and much of it is not usually accessible.

13 The law applies to a very broad category of  
14 information, including not only specific information  
15 collected from a consumer or observed about a consumer,  
16 but also inferences made about a consumer.

17 For example, a data provider may have internal  
18 inferences in analytical modeling systems that  
19 ordinarily cannot be seen by a data provider's  
20 personnel. Will data providers be required to scour  
21 live and backup records to disclose every score that was  
22 produced over a year-long period or disclose individual  
23 analytical variables from modeling systems?

24 For most organizations, this will require  
25 manual searches to gather data from systems that's not

1 even intended to be read by humans. We do not think  
2 that this is helpful to consumers and it's not what they  
3 need or what they want.

4 Without marrying the scope of disclosure,  
5 costs will go up and nonprofits will be hit hard. We  
6 believe the CCPA can be clarified and improved so that  
7 consumers are getting meaningful disclosures and choices  
8 without extreme levels of expense.

9 Second, nonprofits are, and historically have  
10 been, good stewards of personal information. Privacy  
11 and donor trust are priorities to us. To that end, some  
12 parts of the CCPA, from our perspective, are  
13 anti-privacy. The law essentially requires data  
14 providers to start collecting centralized pools of  
15 collective data about consumers and to make disclosures  
16 of those pools of data to requesters who may or may not  
17 be the actual consumer.

18 A privacy-protected practice is to keep  
19 identifying information about a consumer separate from  
20 specific behavior or transaction information. However,  
21 if organizations are expected to very quickly and upon  
22 request provide extensive categories of data, the most  
23 reasonable means of complying will be to collect all of  
24 the data in one place. This creates a new danger. It  
25 makes it easier for security breach to extend a greater

1 level of data about that individual.

2 Additionally, the law requires disclosure  
3 about a consumer within a household to any other  
4 consumer in that household, and this is not always safe.  
5 Someone may have a search history regarding the LGBT  
6 community, but perhaps being out is not safe in that  
7 household.

8 Further, someone in the household may Google  
9 information about abortion or birth control services,  
10 spousal abuse, shelters, or addiction support groups,  
11 and, again, this may not be safe information to disclose  
12 to others in the household.

13 We appreciate and respect the intent of the  
14 CCPA and do not wish to unravel it. The Nonprofit  
15 Alliance is seeking clarification and narrowing the  
16 scope to meaningful information that will benefit the  
17 consumers and thereby reduce the heavy cost on the  
18 impact of data relating to compliance and fix the  
19 elements of the CCPA that contradict privacy such as the  
20 household terms. Thank you.

21 MS. BOOT: Good morning. My name is  
22 Sarah Boot, and I'm here today on behalf of the  
23 California Chamber of Commerce.

24 We are in the process of drafting detailed,  
25 written comments to submit to your office and really

1 appreciate the opportunity to provide this feedback  
2 during this informal period.

3 CalChamber's goal for the AG rulemaking  
4 process is to make sure that CCPA compliance is actually  
5 realistic for all of the businesses; that it covers and  
6 fixes the unintended consequences of this hastily-passed  
7 law, many of which will be harmful to consumers.

8 First, we want to point out this law covers a  
9 massive scope of businesses, far more than most people  
10 realize. In addition to data brokers and larger  
11 companies, the CCPA applies to a third incredibly broad  
12 category of businesses in almost every industry: any  
13 business that annually receives the personal information  
14 of 50,000 or more consumer households or devices. And  
15 that may sound like a high number, but it's not, given  
16 the CCPA's incredibly broad definition of personal  
17 information, which includes all IP addresses and so much  
18 more.

19 For example, CCPA applies to businesses with  
20 50,000 visitors to their website in a year. That  
21 includes ad-supported blogs that may only make a few  
22 hundred bucks in revenue per month. Divide 50,000 by  
23 365 days in a year, the business has an average of 137  
24 unique on-line visitors per day, it's going to hit that  
25 threshold. Just think of all the small businesses that

1 easily conduct an average of 137 transactions per day,  
2 which is about 12 transactions per hour in a 12-hour  
3 day: convenience stores, coffee shops, restaurants. A  
4 lot of these businesses are simply not going to be able  
5 to comply with the CCPA as drafted.

6 Just look at the GDPR. It was recently  
7 reported that over 70 percent of small businesses  
8 covered by that law are not in compliance, and that was  
9 after many years of discussion and ample time to ramp  
10 up. Here, with the CCPA, we are operating on a much  
11 shorter time frame with a law that was passed through  
12 the legislative process in just one week; and that rush  
13 process has resulted in a confusing and complex law that  
14 presents serious privacy concerns and operational  
15 challenges.

16 Today, I am just going to touch on three of  
17 our biggest concerns.

18 First, the CCPA requires businesses to provide  
19 consumers with specific pieces of information that the  
20 business has collected after receiving a verifiable  
21 consumer request. Specific pieces of information is not  
22 defined in the law. It could mean a business must  
23 transmit incredibly sensitive information like credit  
24 card numbers, birthdays, detailed search results back to  
25 the consumer. That creates a risk of an inadvertent

1 disclosure to a fraudster posing as a consumer. And  
2 recall, under CCPA's broad definition of consumer, that  
3 business may have no relationship with the requesting  
4 person.

5 This risk becomes even more heightened given  
6 that third parties can submit consumer requests on  
7 behalf of the consumer. And if this is not addressed,  
8 this is going to cause great consumer harm and it puts  
9 businesses in a catch 22. They could be liable if they  
10 don't respond to a request they find suspicious, but  
11 they can also be liable if they disclose specific pieces  
12 of sensitive information about a consumer to a  
13 fraudster.

14 We request that the AG's office define  
15 specific pieces of information in a way that can limit  
16 these risks. And at a minimum, we request the AG's  
17 office create a safe harbor provision that would remove  
18 liability of a business that complies with the AG's  
19 requirements for verifying consumer requests that  
20 ultimately turns out to be fraudulent.

21 Additionally, although the CCPA states that a  
22 business is not required to relink or reidentify data, a  
23 business can't really provide specific pieces of  
24 information back to a consumer without relinking or  
25 reidentifying that data or match it to a person making

1 the request. This is a glaring inconsistency as the law  
2 is written. As the law is written, it should be  
3 addressed.

4 Second, we have similar concerns with the  
5 CCPA's reference to household and devices in the  
6 definition of personal information.

7 As already mentioned, and as drafted, one  
8 member of a household, whether they are an abusive  
9 spouse or they are a roommate someone barely knows and  
10 they are living with them just to make ends meet, that  
11 person could access all the specific pieces of personal  
12 information for that account, including credit card  
13 information or search histories by another member of  
14 their household. That, obviously, runs counter to the  
15 privacy goals of the CCPA.

16 And, finally, as I've already discussed, CCPA  
17 defines a consumer as any California resident. Without  
18 clarification, that could be interpreted to include  
19 employees. That's obviously problematic for many  
20 reasons. Just one example, an employee accused of  
21 sexual harassment could request that the complaints  
22 about them be deleted. In addition, the operational  
23 costs of including employees and others who do not have  
24 a true consumer relationship with the business, would be  
25 staggering and it would require many businesses to



1 create a whole separate process for those individuals  
2 who are not consumers. It's a separate set of burdens  
3 for people who are not really meant to be included  
4 within the law in this way in their role as employees.

5 I just want to thank you again for creating  
6 this process to allow stakeholders to air concerns. We  
7 obviously have a lot more that we want to discuss and  
8 share with you-all in written comments. We know that  
9 your goal is to protect the consumers and ensure that  
10 compliance is possible, and we truly look forward to  
11 working with you to meet those goals. Thank you so  
12 much.

13 MR. OSWALD: Good morning. Thank you for the  
14 opportunity to provide comments regarding the CCPA's  
15 impacts on consumers and the advertising industry, in  
16 particular, and the digital economy in general.

17 My name is Chris Oswald. I'm Senior VP for  
18 Government Relations at the Association of National  
19 Advertisers.

20 The ANA is the advertising industry's oldest  
21 trade association. Our membership includes nearly 2,000  
22 companies and marketing solutions providers with 25,000  
23 brands that engage almost 150,000 industry professionals  
24 and collectively spend more than \$400 billion in  
25 marketing and advertising annually.

1           Our members include leading marketing data  
2 science and technology suppliers, ad agencies, law  
3 firms, consultants, and vendors. And we also count  
4 among our membership a large number of nonprofits and  
5 charities that will be substantially affected by the  
6 CCPA as we just heard.

7           The ANA supports the underlying goals of the  
8 CCPA. Privacy is an extraordinarily important value  
9 that deserves meaningful protections in the marketplace.

10           As I noted during my remarks at the  
11 January 14th hearing in San Diego, as we look closely at  
12 the CCPA, we are concerned that some of the aspects of  
13 the law will have unintended, adverse consequences for  
14 consumers, businesses, and advertisers that will  
15 inadvertently undermine, rather than enhance, consumer  
16 privacy.

17           During that hearing, I urged you to consider  
18 the following five points in your rulemaking.

19           Number 1, to permit a business to offer  
20 loyalty program -- loyalty-based discount programs that  
21 consumers value and expect without the program  
22 constituting discrimination under the CCPA's  
23 section 1.5.

24           Number 2, recognize that a written assurance  
25 of CCPA compliance is sufficient and reasonable for

1 ensuring the consumer has received, quote, "explicit  
2 notice" and is provided opportunity to exercise the  
3 right to opt out of the sale, the sale of their  
4 information.

5 Number 3, to clarify that businesses may offer  
6 reasonable options to consumers to choose the types of  
7 sales they want to opt out of, the types of data they  
8 want deleted, or to just completely opt out and not have  
9 to just provide an all-or-nothing opt-out --  
10 all-or-nothing opt-out provision.

11 Number 4, to clarify that individualized  
12 privacy policies for each consumer need not be created  
13 in order to disclose the, quote, specific pieces of  
14 personal information the business has collected about  
15 that consumer under section 110(c).

16 And 5, refine the definition of the term  
17 "personal information." Currently, the term creates  
18 tremendous ambiguity around what data is covered by the  
19 law.

20 Today, I add to that list three other  
21 important issues that we urge you to clarify during the  
22 rulemaking process.

23 First, section 140(o)(1)'s definition of  
24 personal information, in combination with 140(g)'s  
25 definition of, quote, "consumer," suggests that the law

1 will treat pseudonymized data in the same manner as data  
2 that could directly identify an individual.

3           However, pseudonymized data does not include  
4 data types that individually identify a person, like  
5 name or E-mail address. Instead, pseudonymized data is  
6 rendered in a manner that does not directly identify a  
7 specific consumer without the use of additional  
8 information. Pseudonymized data, therefore, does not  
9 raise the same privacy concerns as identifiable  
10 information. The CCPA could have the unintended effect  
11 of forcing businesses to associate nonidentifiable,  
12 pseudonymized device data with a specific person seeking  
13 to exercise their rights under the act.

14           This approach would remove existing data  
15 privacy protections enjoyed by California residents  
16 pursuant to the DAA's privacy program.

17           We urge you to distinguish pseudonymized data  
18 from personal information while imposing DAA-like  
19 safeguards against the processing of pseudonymized data.

20           This approach will help ensure California  
21 residents the need to continue to benefit from existing  
22 privacy choices while helping to assure that data  
23 related to their on-line activities does not become  
24 identifiable.

25           Second, in section 140(y) and other sections

1 of the act, allow for a person or an entity that is,  
2 quote, "authorized by the consumer to act on the  
3 consumer's behalf," unquote, to make a deletion or  
4 access request for the consumer under the law.

5 Our concern here is that authorized third  
6 parties who make requests on behalf of consumers appear  
7 to be under no obligation to fully inform those  
8 consumers of the implications of their choices, but they  
9 should be required to inform consumers of the practical  
10 results of making a CCPA request since the business that  
11 will need to comply with the request will not be able to  
12 do so.

13 Without such a requirement, consumers would  
14 not be able to make informed choices in the course of  
15 exercising their rights under the act. Accordingly, ANA  
16 requests that you require authorized third parties that  
17 make CCPA requests on behalf of consumers to communicate  
18 information to consumers about the implications of the  
19 request.

20 And, third, section 105(d)(1) provides an  
21 exception to the deletion right for businesses that need  
22 a consumer's personal information, quote, "in order to  
23 provide a good or service requested by the consumer or  
24 reasonably anticipated within the context of a  
25 business's ongoing business relationship with the

1 consumer," unquote.

2 This language does not clearly place marketing  
3 messages such as subscription renewal reminders within  
4 the purview of the exception. Consumers expect and  
5 value these messages, and so the ANA asks you to clarify  
6 that the deletion exception for providing a service  
7 requested by the consumer, or reasonably anticipated by  
8 the consumer, includes marketing messages such as  
9 subscription renewal reminders.

10 Thank you very much for the opportunity to  
11 speak today. There are a number of other areas of  
12 concern, and the ANA looks forward to submitting  
13 detailed written comments and working with you as you  
14 develop regulations implementing this legislation.  
15 Thank you.

16 MR. CARLSON: Good morning. Thank you for the  
17 opportunity to be here. My name is Steve Carlson. I am  
18 California Government Affairs counsel for CTIA. We are  
19 the trade association for the wireless industry,  
20 including carriers, handset providers, infrastructure  
21 providers, the entire ecosystem.

22 Privacy is essential for consumer trust,  
23 which, in turn, is key for the continued growth of the  
24 mobile ecosystem. Our leadership relative to privacy is  
25 shown by a set of self-regulatory privacy principles

1 that the wireless industry supports and which reflects  
2 its commitment to transparency, consumer choice, data  
3 security, and breach notification.

4 As you have heard throughout these forums, and  
5 again today, what we want to do is make this workable,  
6 not get rid of it.

7 Overly broad and prescriptive privacy laws  
8 could stifle innovation and limit beneficial uses of  
9 data as well as business's ability to deliver services  
10 that consumers demand.

11 We are concerned that the impact on  
12 businesses, consumers, will be negative; that this law  
13 not be anti-privacy, which, unfortunately, we believe in  
14 many ways it is today, and we believe it threatens cyber  
15 security.

16 CTIA urges the Attorney General to use the  
17 authority granted by the act to develop and implement  
18 regulations that bring clarity to the unclear or  
19 ambiguous statutory provisions, which have been  
20 discussed greatly and will continue to be discussed in  
21 which we will point out in our written comments and  
22 regulatory suggestions.

23 Among the things that we believe need to be  
24 addressed, and I think over the course of these forums,  
25 there has sort of been a thread that has run through

1 that point out the most glaring concerns and glaring  
2 flaws with CCPA, including -- I don't want to dwell on  
3 it; I will go into more detail -- but, again, the  
4 definition of consumer, the definitions of personal  
5 information, the fact that personal information has to  
6 be reasonably linkable to an actual person, and clarify  
7 the right to create de-identified aggregate and  
8 pseudonymous information.

9 From the wireless industry standpoint, one of  
10 the issues that is particularly concerning is one that  
11 you have heard about several times already today, which  
12 is bringing the definition of household and devices into  
13 the definition of personal information.

14 We urge the AG to provide guidance on  
15 verifying consumer requests and what constitutes  
16 reasonable efforts to verify and what are acceptable  
17 means of verifying consumers.

18 The Attorney General should consider how to  
19 authenticate other users on the same account who is not  
20 primary -- who are not the primary account holder, as is  
21 typically the case for our family plans.

22 The current text can be interpreted to allow a  
23 consumer to request an extensive set of personal  
24 information about his or her spouse as a member of the  
25 household, potentially compromising the privacy and



1 safety of the spouse. A similar situation might occur  
2 in the case of roommates or other family members. We  
3 think this is very concerning, very dangerous, and  
4 absolutely has to be addressed.

5 So we are looking forward to working with the  
6 AG. The AG has as important a role in these regulations  
7 as I have seen in my many years in the regulatory  
8 process. I know you are taking this very seriously and  
9 you are spending an incredible amount of time and  
10 attention in listening to those who have issues that we  
11 think are very rational and important ones to look at,  
12 and we look forward to continuing to work with you and  
13 appreciate the opportunity.

14 MR. TERRAZAS: Good morning. My name is  
15 Christopher Terrazas, and I am the creative director at  
16 3Fold Communications here in Sacramento. I am also  
17 representing the American Advertising Federation. I'm  
18 the governor of Northern California, and I am just  
19 generally a nice guy.

20 We have been operating in Sacramento,  
21 California, for nearly 25 years, and although our  
22 business primarily involves advertising, consumer data  
23 is crucially important to our competitiveness and  
24 growth. This data is used to personalized and improve  
25 product and service offerings to find new business

1 partners and to reach out to potential customers. We  
2 take enormous pride in responsibly handling this data  
3 for the benefit of our customers, and our businesses  
4 have limited means to verify the legitimacy of consumer  
5 requests under the CCPA.

6 The California Consumer Privacy Act 2018  
7 increases the risk of fraud. This issue is particularly  
8 troublesome, because the CCPA allows third parties,  
9 including third party businesses, to make requests for  
10 consumers. Our customers' businesses will have trouble  
11 determining which requests are legitimate and which are  
12 fraudulent. This puts consumers and data about  
13 consumers at risk, and makes it harder for us to protect  
14 our customers' business's data from unauthorized  
15 requests.

16 We request -- we request -- that the  
17 Attorney General provide -- one, provide flexibility for  
18 businesses to verify consumer requests; and two, provide  
19 increased transparency to consumers.

20 The Attorney General should recognize that  
21 verifying consumer requests may take many different  
22 forms and should refrain from enforcement actions when  
23 companies make commercially reasonable efforts to verify  
24 a consumer.

25 In cases where a third party intends to make a

1 CCPA deletion or opt-out request on behalf of a  
2 consumer, the third party should first be required to  
3 make the consumer aware of the impact of the consumer's  
4 deletion or opt-out request, such as no longer receiving  
5 information on new offers.

6 This notification requirement is important,  
7 because the businesses that ultimately must comply with  
8 the request will not be able to directly discuss these  
9 impacts with the consumer who has a right to understand  
10 the implications of their request.

11 The CCPA removes basic, needed, nonsensitive  
12 data from the marketplace that we rely upon and creates  
13 competitive disadvantages for California businesses.  
14 Small businesses rely upon consumer data to improve  
15 products and services and to find new customers and  
16 business partners.

17 When a customer makes a deletion request, our  
18 customers' businesses, as a small business, will suffer  
19 more than larger companies because of the smaller size  
20 of our customers' business's customer list. The CCPA  
21 advantages out-of-state businesses of equal size and  
22 nature of small businesses in California who do not meet  
23 the threshold requirements for covered businesses.  
24 These out-of-state businesses will not have to create  
25 new compliance regimes, including incurring significant

1 legal fees and technology costs.

2 Similarly -- I always have a hard time with  
3 that word -- those businesses will not face potentially  
4 business-destroying funds in the event of a data breach.  
5 Complying with the law will be incredibly expensive for  
6 our customers' businesses. This added expense will  
7 limit our customers' businesses from hiring new  
8 employees and from expanding our customers' businesses  
9 in general. Consumer will suffer and receive less  
10 privacy protections.

11 We request that the Attorney General provide  
12 flexibility for small businesses where consumer requests  
13 are cost-prohibitive. It will be very expensive for our  
14 customers' businesses to comply with the consumer  
15 requests because of the broad definition of personal  
16 information. The CCPA already recognizes that a  
17 business may charge a reasonable fee or refuse to act on  
18 a consumer request when consumer requests are manifestly  
19 unfounded or excessive. The AG should interpret  
20 "excessive" to include requests that are unreasonably  
21 costly relative to the size of the business.

22 Thank you very much for letting me speak. I  
23 am honored to be a part of this process. Thank you.

24 MR. ISBERG: Good morning. My name is  
25 Pete Isberg. I serve as president of the National

1 Payroll Reporting Consortium, which is a trade  
2 association of whose members and organizations provide  
3 payroll processing services to nearly 2 million U.S.  
4 employers, over 36 percent of the private sector  
5 workforce. I'm also here representing the American  
6 Payroll Association, which is a nonprofit association  
7 representing over 20,000 payroll professionals across  
8 the United States.

9 I have written testimony, but I'll summarize  
10 this here.

11 Privacy and protection of personal data are of  
12 paramount concern to payroll service providers and  
13 payroll administrators. We applaud the objective of the  
14 legislation and the efforts of policymakers to establish  
15 appropriate and balanced legislation that effectively  
16 protects consumers without unduly impeding the critical  
17 functioning of appropriately-protected business  
18 activity.

19 Our comments today are intended to highlight  
20 the ambiguous and overly broad definitions and terms of  
21 the law, and to point out a number of practical  
22 implications, and to seek clarity in related  
23 regulations.

24 The CCPA creates new rights for California  
25 residents to access the personal information maintained

1 by the business, to have such information deleted, and  
2 to opt out of the sale, in other words, transfer of  
3 their personal information.

4 Our greatest concern is that the broad,  
5 ambiguous definition of sale and personal information  
6 and consumer could result in inconsistent implementation  
7 of the law.

8 There is widespread confusion and inconsistent  
9 analyses over whether employment records in the  
10 employment context generally are regulated by the CCPA.  
11 You know, someone argued that it conflicts with existing  
12 legal obligations and, again, this may result in  
13 inconsistent application of privacy protections.

14 We recommend that regulations clarify these  
15 definitions and establish exceptions necessary to  
16 eliminate ambiguity.

17 A couple of examples, the right to opt out of  
18 any sale could prevent the normal functioning of routine  
19 business operations, including employer payroll  
20 operations. The CCPA defines sale to include any data  
21 transfer for monetary or other valuable consideration.  
22 It's not clear whether the monetary consideration must  
23 be received for the purchase of personal data as opposed  
24 to some other business arrangement where the data is not  
25 the subject of the exchange. Again, the example of

1 payroll administration, could an employee inadvertently  
2 block the subsequent transfer of their information for  
3 payroll processing? Nobody would want to probably, but  
4 they might inadvertently issue a broad block or  
5 do-not-sell order that would be interpreted that way.

6 Businesses also change information and  
7 pay-related fees to third parties for other services,  
8 for example, to prevent fraud for money laundering  
9 screening, identity protection functions, or identity  
10 verification functions and benchmarking activities.

11 In terms of the right to access, we noted that  
12 employees already have the right to access their  
13 personal files and records. But the definition of  
14 personal information could relate to a consumer, or has  
15 been noted this morning, a household. Inclusion of  
16 household in that definition could be read to allow a  
17 spouse to gain access to critical, sensitive employment  
18 records.

19 In terms of the request -- right to request  
20 that personal information be deleted, this would  
21 conflict with many federal and state laws. For example,  
22 California Labor Code requires employers to maintain  
23 detailed records reflecting virtually all activity with  
24 respect to employment, from hiring, enrollment in  
25 benefits, documentation of hours worked, wages earned,

1 deductions from pay, and many other related matters. It  
2 would be very problematic if any employer was led to  
3 actually delete records under the CCPA.

4 Similarly, federal and state laws require  
5 employers to maintain detailed records of every wage  
6 payment, amounts withheld, quarterly wage reports, W-2,  
7 IRS, and employment tax returns, and so on. Employers  
8 must be able to substantiate virtually all such activity  
9 and, therefore, any request for deletion of employment  
10 records would be limited to records not required by law.  
11 But if it's not entirely clear to everyone in the room,  
12 some employers might be led to incorrectly delete  
13 employment records, so we are looking for clarity here.

14 One concern that we noted is that an employee  
15 determined to, for example, having engaged in sexual  
16 harassment could opt out from effective screening  
17 mechanisms or ask for deletion of critical employment  
18 records. Actual findings of harassment should obviously  
19 be preserved in performance records.

20 So, in closing, we believe that broad  
21 definitions might result in inconsistent application of  
22 the law, which in turn could defeat its purpose. We  
23 urge the Attorney General's office to clarify these  
24 points during rulemaking. Again, we support  
25 California's commitment to protecting the privacy and



1 security of personal data and appreciate this  
2 opportunity to offer comments.

3 MR. ELLMAN: Good morning. My name is  
4 Eric Ellman. I'm the Senior Vice President of Public  
5 Policy and Legal Affairs for the Consumer Data Industry  
6 Association, CDIA.

7 CDIA, as a trade association, is representing  
8 over 100 consumer reporting agencies, including the  
9 nation's leading credit bureaus -- Equifax, Experian and  
10 TransUnion -- and 100 other or so data companies that  
11 provide a variety of risk management products and  
12 services for their business, government, law  
13 enforcement, and nonprofit consumer customers, including  
14 things like criminal background checks, mortgage  
15 reporting, tenant screening, and things like that.

16 Our members are often third parties without  
17 direct contact with consumers. We provide fraud  
18 prevention, authentication, and other services to make  
19 transactions flow smoothly for law enforcement,  
20 businesses, nonprofits, and volunteer organizations.

21 We have four specific concerns that I want to  
22 bring to you this morning, and we will follow up in  
23 detail with written comments probably by the end of this  
24 month.

25 First, I want to address fraud prevention

1 services; second, third party notice requirements;  
2 third, commercial credit reporting; and fourth, some  
3 other interoperable or other operability concerns that  
4 we have with the statute.

5 First, on fraud prevention services, I know  
6 that your office has heard a lot on the need for  
7 personal information for fraud prevention from the first  
8 party perspective, companies that deal directly with  
9 consumers. CDIA members are regularly third party  
10 providers of fraud prevention services, and the Office  
11 of the Attorney General should consider our unique role  
12 in preventing fraud against businesses, government, and  
13 nonprofits. Since the CCPA provides consumers the right  
14 to request a deletion and/or opt out of sharing personal  
15 information, that is included in fraud prevention tools  
16 that might be deleted from or prevented from being  
17 shared.

18 We hope the Attorney General's office will use  
19 its statutory authority to clarify, through rulemaking,  
20 that the CCPA fraud exemption to the deletion of data  
21 covers services that might be designated or designed to  
22 prevent fraud.

23 Second, third party notice requirements:  
24 Section 1798.115(d) of the act prohibits third parties  
25 from selling personal information about a consumer that

1 has been sold to third parties by a business, unless the  
2 consumer has received an explicit opt-out notice. Third  
3 parties, like our members, often do not have a direct  
4 relationship to consumers whose personal data is held,  
5 and as a result of that lack of direct business  
6 relationship, these third parties are not able to  
7 provide direct notices to consumers. This is an  
8 unintended consequence as a result of the CCPA, which  
9 the Attorney General has the power to correct. As a  
10 result of this, incidental obligation of data transfers  
11 may be unnecessarily and unintentionally cut off.

12 We request that the AG's office make clear,  
13 through its rulemaking, that a third party may rely on  
14 its own privacy policies and written attestations from  
15 data providers to comply with 1798.115(d).

16 Third, commercial credit reporting: Several  
17 CDIA members provide commercial credit information,  
18 which is regulated into a separate provision of  
19 California law related to, separate, and apart from the  
20 Consumer Credit Reporting Agencies Act.

21 The Attorney General should use its authority  
22 to clarify, through rulemaking, that the term "consumer"  
23 in the CCPA excludes business persons contained in the  
24 commercial credit reports and related business  
25 information.

1           Now turning to some more specific, other  
2 interoperability concerns, a number of people have  
3 questioned and sought clarification on the definition of  
4 a household. We are in that same position. The  
5 definition of a household needs adjustments since nobody  
6 wants businesses to disclose all of the data associated  
7 with an address to any individual ever associated with  
8 that address. We ask that the AG provide clarity on the  
9 phrase "not incompatible with" with respect to public  
10 records exceptions and the data collection of personal  
11 information. Our members regularly use public  
12 information to help prevent fraud, locate victims,  
13 witnesses, fugitives, and other services on behalf of  
14 government and law enforcement and the private sector.

15           We ask the AG's office to propose a safe  
16 harbor or statement that third parties, including those  
17 that did not meet the definition of a business, are not  
18 liable without actual knowledge of the consumer's  
19 opt-out.

20           We request clarity that inferences drawn from  
21 any personal information to create a consumer profile is  
22 not personal information when the personal information  
23 upon which the inference is to be drawn have been  
24 de-identified and de-aggregated. Those are, again,  
25 similar comments that you have heard throughout.

1           Our 100 or so consumer reporting agency  
2 members are very heavily-regulated, enforced,  
3 supervised, and examined by a variety and a combination  
4 of a number of federal and state laws: The Federal Fair  
5 Credit Reporting Act, the California Credit Reporting  
6 Act, the Gramm-Leach-Bliley Act --

7           (Interruption by the Reporter.)

8           THE HEARING OFFICER: Slow down.

9           MR. ELLMAN: Sorry. I'm a New Yorker. I tend  
10 to talk a little fast. I apologize.

11           We are regulated, supervised, enforced, and  
12 examined by a variety of federal statutes and rules and  
13 agency regulations. We are supervised, enforced, and  
14 examined by the Federal Fair Credit Reporting Act, the  
15 California Credit Reporting Act, the federal  
16 Gramm-Leach-Bliley Act, the Safeguards Rule of the  
17 Federal Gramm-Leach-Bliley Act, the CFPB, the FTC, all  
18 have a hand in supervision, regulation of our industry,  
19 as well as enforcement capabilities from the FTC, the  
20 CFPB, and the State Attorney General, as well as private  
21 rights of action.

22           We are a very heavily-regulated industry. We  
23 want to work with you to try to make the CCPA work where  
24 it can, but there are places where there are significant  
25 inconsistencies and problems, which ultimately will have

1 a negative impact on fraud prevention, law enforcement,  
2 and risk management for all people, not just in  
3 California, but in the country as a whole.

4 I thank you for your time and attention, and  
5 we look forward to providing you with written comments,  
6 and we are happy to be available for any questions that  
7 you may have. Thank you.

8 MR. MATTOCH: Good morning. Mike Mattoch,  
9 M-a-t-t-o-c-h, on behalf of counsel for Consumer  
10 Watchdog.

11 Let's try to put this into perspective. An  
12 overwhelming majority of Americans report that they are  
13 worried about the security of their personal data  
14 companies collect on them. 85 percent of Americans  
15 consistently say that they want to control the data that  
16 is collected about them.

17 The California Consumer Privacy Act is the  
18 first law in the nation that makes that promise. Your  
19 mission impossible, since you have been forced to accept  
20 it, is to make sure that that promise is kept.

21 24 million financial documents for tens of  
22 thousands of loan and mortgage customers from the  
23 nation's largest banks has been disclosed. Everything  
24 an identity thief needs to impersonate a person was  
25 exposed in a breach. Marriott disclosed a breach of

1 400 million of its customers, including passport numbers  
2 and credit card. Facebook recently revealed another  
3 major breach of public trust, admitting that it gave  
4 major tech companies greater access to use data than  
5 they previously disclosed.

6 I'm going to work in reverse descending order  
7 up there, because I think financial incentives may be  
8 the most important thing you have to look at.

9 The law is clear, the right of Californians to  
10 equal service and price, even if they exercise their  
11 privacy rights. There cannot be a denial of goods or  
12 services for a consumer who opts out. Any incentives  
13 provided by companies to convince consumers to allow  
14 data sales cannot force mid- to low-income people and  
15 consumers to give up their privacy in order to use a  
16 website or service. That means any different price or  
17 disparate level of service must be connected to the  
18 value of the consumer's data.

19 The only way to do that so the AG and the  
20 public can be confident that companies aren't  
21 discriminating against consumers who choose privacy is  
22 to require disclosure of actual revenues or other method  
23 by which a company calculates value of the data to the  
24 AG and to the public. Regulations should require  
25 companies to submit quarterly reports to the AG. When a

1 consumer is offered explicit -- is offered a financial  
2 incentive not to opt out, the website must be explicit  
3 as to how it is calculated. Companies must prove the  
4 charge is correlated to the value of the consumer's  
5 data.

6 Opt-out: Must give consumers a clear and  
7 obvious choice, not the got-to-get-to-the-thing thing we  
8 already do right now on our iPhones. It has to be  
9 explicit, and it has to prohibit multiple levels of  
10 hurdles and legalese in between a consumer's first click  
11 to opt out and actually implementing that right. The  
12 law also requires a link that says, "Do not sell my  
13 personal information" in bold type.

14 The right to download: The ability to  
15 download your data and move it to another service is  
16 essential for individual control of the data.

17 Have heard that there are industry compliance,  
18 that this right needs to be limited or narrowed because  
19 it's too burdensome. I discount that right out of hand  
20 since the right has already been successfully  
21 implemented in Europe under the GDPR, so it is clearly  
22 possible.

23 Unique identifiers: The law is clear that IP  
24 is a unique identifier, and that personal information  
25 includes anything capable of being associated with or



1 reasonably linked, directly or indirectly, with a  
2 household, consumer, or family. There is zero  
3 justification for excluding IP address since it can  
4 easily be linked to a specific person or household.

5 Categories of information: The law defines  
6 personal information broadly as all data a company  
7 collects and relates to a person in any way. Namely,  
8 since companies can make even seemingly innocuous data  
9 broad, you should reject any effort to limit the kinds  
10 of personal information the law applies to. And as much  
11 as I love my profession, there should be no legalese.

12 And, finally, if there is a value to a company  
13 sharing or selling it, there is a value to consumers  
14 opting out of its sale. Consumers who opt out of sale  
15 sharing will expect that info also to be protected and a  
16 right to sue when it is not. We will be submitting  
17 written information more detailed, but thank you very  
18 much for your time.

19 MS. SMITH: Good morning. My name is  
20 Heather Smith and I'm the president of the American  
21 Advertising Federation, Sacramento Chapter here, as well  
22 as the lieutenant governor for District 14, which  
23 comprises all of Northern California and Reno.

24 The AAF represents thousands of companies from  
25 small businesses to household brands across every

1 segment of the advertising industry, including a  
2 significant number of California businesses. In our  
3 local club, we have over 100 small-, medium-, and  
4 large-sized businesses from ad agencies to media  
5 outlets.

6 Our members engage in responsible data  
7 collection and use that benefit -- and use to benefit  
8 consumers and the economy. We believe privacy deserves  
9 effective protection in the marketplace.

10 We strongly support the objectives of the  
11 California Consumer Privacy Act, but have notable  
12 concerns around the likely negative impact on California  
13 consumers and businesses from some of the specific  
14 language in the law. I am here today to provide you  
15 with information about the significant importance of a  
16 data-driven and ad-supported on-line ecosystem, industry  
17 efforts to protect privacy, and draw your attention to  
18 several areas that can be addressed and improved through  
19 the rulemaking process.

20 Number 1, the data-driven and ad-supported  
21 on-line ecosystem benefits consumers and fuels economic  
22 growth. The free flow of data on-line fuels the  
23 economic engine of the Internet creating major consumer  
24 benefit. For decades on-line, data-driven advertising  
25 has powered the growth of the Internet by funding

1 innovative tools and services for consumers and  
2 businesses to connect and communicate. Data-driven  
3 advertising supports and subsidizes the content and  
4 services consumers like you and I expect and rely on,  
5 including video, news, music, and much more, at little  
6 or no cost to the consumer.

7 Companies also collect data for numerous  
8 operational purposes, including ad delivery and  
9 reporting, fraud prevention, network enhancement, and  
10 customization. These uses are necessary for a seamless,  
11 cross-channel, cross-device consumer experience and a  
12 functioning digital economy.

13 As a result of this advertising-based model,  
14 the Internet economy in the U.S. has rapidly grown to  
15 deliver widespread consumer and economic benefits.

16 According to a recent study conducted for the  
17 Interactive Advertising Bureau, the IAB, by Harvard  
18 Business School professor, John Deighton, the U.S.  
19 ad-supported Internet created 10.4 million jobs in 2016.  
20 The data-driven ad industry contributed -- I was shocked  
21 by this number -- \$1.121 trillion to the U.S. economy  
22 that year, doubling its contribution over just four  
23 years and accounting for 6 percent of the U.S. domestic  
24 product.

25 Consumers have enthusiastically embraced the

1 ad-supported model, and they have actively enjoyed the  
2 free content and services that it enables. They are  
3 increasingly aware that those services are enabled by  
4 data collected about their interactions and behavior on  
5 the web and in mobile applications and they support the  
6 exchange value.

7 In fact, a Zogby survey commissioned by the  
8 Digital Advertising Alliance found that consumers  
9 assigned a value of nearly \$1,200 to common ad-supported  
10 services like news, weather, video content, and social  
11 media. A large majority of survey consumers --  
12 85 percent -- stated that they liked the ad-supported  
13 model, and 75 percent indicated that they would greatly  
14 decrease their engagement with the Internet were a  
15 different model to take place.

16 Our members have long been champions of  
17 consumer privacy. Consumer trust is vital to our  
18 members' ability to successfully operate in the  
19 marketplace, and they take that responsibility seriously  
20 by engaging in responsible data practices.

21 A primary example of this commitment is  
22 through the Digital Advertising Alliance YourAdChoices  
23 program.

24 The DAA created and enforces a self-regulatory  
25 code for all companies that collect or use data for

1 interest-based advertising based on practices  
2 recommended by the Federal Trade Commission and its 2009  
3 report on on-line behavior on advertising.

4 The principles in that code provide consumer  
5 transparency and control regarding data collection and  
6 use of web viewing data, application use data, and  
7 precise location data.

8 Importantly, the YourAdChoices program and the  
9 DAA principles are a novel kind of industry-led  
10 initiative whereby all companies engaging in the  
11 described practices are subject to established privacy  
12 safeguard obligations.

13 Also, the DAA principles are independently  
14 monitored and enforced. To date, more than 90  
15 compliance actions have been publicly announced.

16 The DAA principles include rules around the  
17 collection and use of web viewing data for advertising  
18 and restrictions for purposes beyond advertising, strong  
19 prohibitions on the use of such data for eligibility  
20 purposes for employment, insurance, credit and  
21 healthcare treatment, and detailed guidance around the  
22 applications of the principles in the mobile and  
23 cross-device environments. Most recently, it would  
24 provide users with increased transparency about the  
25 source of the political advertising they see on-line.





















1 infringement, or may impair our members' ability to  
2 prevent harassing or otherwise illegal conduct with the  
3 on-line community of gamers.

4           Verifying that a company is interacting with  
5 the account holder and not an imposter is an important  
6 predicate to honoring the various consumer requests  
7 contemplated under the law. Many games and game  
8 services require the user to establish a  
9 password-protected account for purposes of managing  
10 various aspects of the user experience. We would like  
11 to see a clarification that account registration is a  
12 permissible means of verifying consumers' identity.

13           We also believe that where a good or service  
14 cannot be provided without the requested data, it should  
15 be permissible to deny a consumer that good or service.

16           Game publishers need the flexibility to have  
17 different business models to be able to develop  
18 high-quality, engaging video game content while also  
19 serving the game audience -- sorry -- the full audience  
20 of gamers, for example, ad-supported games or  
21 free-to-play games. Enabling the consumer to opt out of  
22 data sharing while still guaranteeing them access to the  
23 service would jeopardize the industry's ability to offer  
24 a free experience.

25           Thank you for your time and attention to these

1 important issues for both consumers and companies alike.

2 MS. KLOEK: Hello. My name is Sara Kloek, and  
3 I am the Director of Education Policy at the Software  
4 and Information Industry Association. I'll speak slow,  
5 because I work in the realm of education.

6 We represent education technology companies  
7 that work with schools to provide students with digital  
8 learning experiences, help teachers record grades and  
9 attendance, and help administrators develop school bus  
10 schedules.

11 I am here today to talk about the impact that  
12 the CCPA has on the educational sector. As currently  
13 drafted, a 16-year-old California student may have the  
14 right to delete all of their grades without the  
15 knowledge of their parent or public school.

16 Even before the passage of CCPA, there was a  
17 comprehensive framework of privacy laws regulating the  
18 information that education technology companies may  
19 collect or maintain about students and how they may use  
20 it, starting with the Family Educational Rights and  
21 Privacy Act in 1974, and more recently, laws such as the  
22 Student On-Line Personal Information Protection Act of  
23 2014, and AB 1584, directly regulating education  
24 technology companies providing services to schools,  
25 student privacy laws are either as strict or stricter



1 than the requirements set forth by CCPA.

2 For instance, prior to the passage of CCPA,  
3 education and technology companies were banned from  
4 selling students' personal information, parents and  
5 eligible students had the right to request access and  
6 amend education records, and were limited through both  
7 law and contractual requirements on what could be done  
8 with student data.

9 CCPA makes compliance with student privacy  
10 laws more confusing. It is unclear how a vendor  
11 servicing a contract to a school, state, or local  
12 government will need to comply with CCPA.

13 The deletion rights under CCPA could cause  
14 major compliance confusion and should be clarified.

15 Additionally, state requirements for school  
16 record retention and federal requirements for school  
17 control of education data disclosed to vendors may prove  
18 difficult to follow if CCPA remains as written.

19 I urge the Attorney General to clarify that  
20 businesses need not breach student privacy laws to  
21 comply with CCPA. Thank you for your time.

22 MR. PROPES: Hello, and thank you for the  
23 opportunity to speak with you today. My name is  
24 Alex Propes, and I work with the Interactive Advertising  
25 Bureau, or IAB.

1           Founded in 1996, the IAB represents over 650  
2 leading media and technology companies that are  
3 responsible for selling, delivering, and optimizing  
4 digital advertising campaigns. Working with our member  
5 companies, IAB develops technical standards and best  
6 practices and fields research in interactive  
7 advertising. We are committed to professional  
8 development and elevating the knowledge, skills,  
9 expertise, and diversity of the industry's workforce.

10           Of our 650 member companies, nearly 200 are  
11 headquartered across California from San Diego to  
12 San Francisco. Our California-based member companies  
13 include newspapers, media companies, on-line shopping  
14 networks and retailers, and technology companies. All  
15 of these services are supported by revenues from on-line  
16 advertising; and our industry supports over 478,000  
17 full-time jobs across the state and contributes  
18 \$178 billion to the California GDP based on research we  
19 have conducted at Harvard Business School.

20           We believe the effective privacy regulation  
21 that promotes consumer trust and builds on industry best  
22 practices can and should promote even greater job  
23 creation, economic growth in California, and it's in  
24 this spirit that we provide feedback today.

25           We support the guiding principles of

1 transparency, control, and accountability that are  
2 captured in the CCPA, and we agree that we need simpler,  
3 more understandable opt-outs from the use of data within  
4 our industry. And it's in furtherance of that mission  
5 that we have created the Digital Advertising Alliance  
6 and continue to develop and evolve this program over  
7 time.

8 As we have heard earlier today, the DAA is the  
9 industry cross and self-regulatory privacy -- it offers  
10 cross-industry self-regulatory privacy principles, which  
11 have been widely implemented across the digital  
12 advertising industry and are a requirement for companies  
13 wishing to join the IAB.

14 While the CCPA seeks to enshrine these  
15 important concepts, we are concerned that, without  
16 additional guidance and clarification from the Attorney  
17 General, the law could result in unintended  
18 consequences.

19 Today, I would just like to highlight a few  
20 issues of relevance in the media and marketing  
21 industries as they work towards CCPA compliance.

22 First, it is important that CCPA's  
23 nondiscrimination provisions do not prevent publishers  
24 from charging a reasonable fee as an alternative to  
25 using an advertising-supported business model. There is

1 concern that the CCPA nondiscrimination provisions would  
2 prevent publishers, including small publishers and our  
3 members, from charging a fee to access their content for  
4 consumers that elect to opt out. Publishers rely on  
5 third party advertising providers to generate revenue to  
6 support their content and services, and so it's critical  
7 that we avoid requiring businesses and websites to grant  
8 everyone access to their visual sites, even those  
9 visitors who have opted out, without allowing for some  
10 paid alternative.

11 Second, it is important that CCPA provide  
12 businesses with the flexibility to offer reasonable  
13 options to consumers with regard to deletion and opt-out  
14 rights. Considering the breadth of the definition of  
15 sale, and the number of activities that are captured by  
16 an opt-out, we believe it is beneficial to both  
17 consumers and businesses to be able to offer reasonable  
18 options for the opt-out.

19 Third, it is important that CCPA provide the  
20 needed flexibility for businesses to verify consumer  
21 requests. In many scenarios in the digital advertising  
22 industry, businesses have limited ability to verify the  
23 legitimacy of consumer requests under the CCPA. This  
24 difficulty in determining which requests are legitimate  
25 and which are fraudulent puts consumers and their data

1 at risk from unauthorized requests. So we would ask  
2 that the Attorney General recognize that verifying  
3 consumer requests may take many forms, and we would also  
4 ask that the Attorney General distinguish between  
5 parties that hold data that is purely pseudonymous and  
6 that have no means of connecting it to an actual person.

7 Thank you again for the opportunity to speak  
8 today, and we look forward to providing more detailed  
9 written comments with the Attorney General in the days  
10 ahead.

11 MR. PAGE: Good morning. My name is  
12 Craig Page. I'm with the California Land Title  
13 Association. I'm executive vice president and counsel  
14 for the industry. The title industry is comprised of  
15 both --

16 (Interruption by the Reporter.)

17 MR. PAGE: I represent the California Loan  
18 Title Association. We represent both the California  
19 underwritten title companies and title insurers  
20 throughout the state.

21 We've worked closely with the AG in the past  
22 on the electronic record recording delivery system  
23 regulations and we look forward to working closely with  
24 you in this year as well.

25 Part of the process of providing title

1 insurance and serving our customers in California in  
2 transactions require the title search of county records  
3 and also a search of judgment records, past collected  
4 records, and other information that's publicly  
5 available. And in that process, we identify a number of  
6 outstanding financial encumbrances that are of record.  
7 Some of those are very important.

8 And I strongly support the Chamber in other  
9 comments that were made earlier, but I'm also going to  
10 focus more on unintended consequences that I think that  
11 were not considered when the legislation was crafted.

12 I think that there are some carve-outs  
13 relating to publicly-available information. There is  
14 some information -- there is some latitude on fraud, but  
15 I think that as you guys are drafting your regulations,  
16 we would like to have a real focus on those things.

17 The title industry, as we define liens and  
18 find liens of record, we find child support liens, which  
19 are abstracts of support that are out there. Through  
20 the information given to us by the California Child  
21 Support Collection Services Agency, the industry  
22 collects anywhere from \$15- to \$20 million a year in  
23 child support. These are liens that are of record, and  
24 these are often deadbeat parents who are trying to avoid  
25 payment of these liens. They try hard not to be tracked

1 down, and the information that we pull out of abstracts  
2 of support that are of record often are drivers license,  
3 the deadbeat parent's last known address, truncated  
4 Social Security numbers. There is a number of things  
5 that are out there that we need to have access to.

6 And people who are trying to avoid tax liens  
7 and trying to avoid child support liens or other  
8 financial encumbrances or judgment liens, they are  
9 trying to lay low. They want to exercise their option  
10 to opt out of information collected about them. They  
11 want to have information deleted about them.

12 The title insurance industry plays a very  
13 important role in that we thwart fraud all the time. We  
14 work with financial -- we work with federal agencies,  
15 like FinCEN and some other agencies, that are looking  
16 for money laundering and ask us to collect information  
17 in the escrow process to ensure that it's not happening.  
18 Not only do we collect it, but we are also, by many  
19 federal agencies, required to maintain it for several  
20 years so that we have this data available if a fed wants  
21 to audit or go through records.

22 So we work closely with the federal agencies;  
23 we work closely with DAs at a local level. We often  
24 will discover fraudulent transactions or things that  
25 look hinky -- that's a legal term, I believe -- and we

1 flag it and work with DAs all the time.

2 So we think that the DA -- Attorney General's  
3 office, as you're looking at this, concentrate on making  
4 sure that the publically-available information is  
5 maximized, because those documents are supposed to be  
6 provided constructive notice and provide as much  
7 information to people as possible.

8 We also want to make sure that our ability to  
9 work with federal agencies, state agencies, local  
10 government, won't be impaired so that we can share  
11 information. Title industry shares information between  
12 companies to thwart fraud all the time. And as we  
13 generate policies, we collect child support and billions  
14 of dollars in government taxes every year, not because  
15 we are required to by law, but because it's part of the  
16 service that we provide to lenders and consumers,  
17 because if that money is not collected, it becomes their  
18 obligation if they buy the property.

19 So we look forward to working closely with  
20 you. And, again, we support many of the issues that  
21 were raised by other speakers in the Chamber of Commerce  
22 about other business-related issues, and I will also be  
23 supplying detailed comments to you as well. Thank you.

24 MR. HARRISON: Good morning. I am  
25 James Harrison. I'm an attorney at



1 Remcho, Johansen & Purcell, and I'm here today on behalf  
2 of Californians for Consumer Privacy, which was the  
3 proponent of Californians for Consumer Privacy Act.

4 First, I would like to thank you for your  
5 efforts to draft regulations to implement the CCPA. I  
6 know you have a complicated task and we appreciate it.  
7 We also appreciate your long-standing efforts to protect  
8 Californians' privacy and to hold businesses accountable  
9 when they fail to protect consumers' personal  
10 information.

11 We have heard a lot of detailed concerns about  
12 the CCPA this morning. So I think it's important to  
13 take a step back and remember that one of the Attorney  
14 General's most important tasks is to ensure and protect  
15 the four pillars of the CCPA as it goes about drafting  
16 regulations.

17 Those include the right of Californians to  
18 learn what information the business has collected about  
19 them and how they use it, the right to tell a business  
20 not to sell their information, the right to request that  
21 a business delete information that it has collected from  
22 the consumer and, importantly, the prohibition on  
23 businesses against discriminating against a consumer who  
24 has exercised one of those rights.

25 From our perspective, there are three top

1 priorities for your task in drafting regulations.

2 First, as we have heard today, it's incredibly  
3 important that consumers have an easy and clear way to  
4 opt out of the sale of their personal information. This  
5 means an opportunity to opt out on a global level  
6 regardless of whether other opportunities are offered to  
7 opt out of the sale of particular pieces of information.  
8 There must be an opportunity that's clear and easy to  
9 opt out of the sale of all of your personal information.

10 Second, we think it's critical that the  
11 Attorney General adopt regulations around the submission  
12 of a verifiable consumer request to ensure that a  
13 consumer has the opportunity to request access to  
14 information, but that that request be authenticated by,  
15 among other means, a password-protected account,  
16 dual-factor authentication, or challenge response, or  
17 some other method that ensures that the business has an  
18 opportunity to verify that the consumer who is making  
19 the request is the consumer about whom the business has  
20 collected information.

21 And, finally, it is critically important that  
22 the regulations ensure that we do not create a  
23 pay-for-privacy system in the state of California.  
24 Financial incentives and discounts offered by businesses  
25 should be tied to the average value to the business of

1 consumers' data. We think that's a way to ensure that  
2 loyalty programs can continue while also preventing  
3 businesses from charging consumers unjust or  
4 unreasonable rates and fees for exercising their privacy  
5 rights.

6 Thank you very much for your attention. We  
7 appreciate all of your efforts.

8 MR. HAWKS: Excuse me. Thank you. My name is  
9 Jack Hawks, H-a-w-k-s. I'm the executive director of  
10 the California Water Association.

11 I actually hadn't planned to speak today,  
12 obviously, but I did want to bring up one aspect of the  
13 CCPA that hasn't been discussed, and it concerns the  
14 members of my organization.

15 CWA, or the California Water Association,  
16 represents about 100 water -- drinking water utilities  
17 that provide water service to about 6 million  
18 Californians all over the state. We are regulated by  
19 the California Public Utilities Commission. And our  
20 concern, or principal concern at this point in time, is  
21 that the ambiguous language and some of the conflicting  
22 language in the statute, CCPA's statute, will conflict  
23 with the PUC's -- the Public Utility Commission's -- own  
24 privacy rules to which we are subject.

25 Right now, our utilities do not collect data

1 on their customers unless mandated to do so by the PUC  
2 for a business reason, and at this one time, there are  
3 basically two business reasons. One is to obviously  
4 provide, in our case, the water utility service, but  
5 also to provide an opportunity for our customers to get  
6 a discount on their utility bills. And so information,  
7 customer information, is needed for those two purposes.

8 The PUC's privacy rules do not allow us to  
9 sell data to anybody. But as I have come to learn,  
10 there are many aspects in the CCPA to which the  
11 regulated utilities will be subject. And our request at  
12 this point in time is just that the AG's office work  
13 with the regulated utilities and the Public Utilities  
14 Commission to coordinate the implementing regulations of  
15 the CCPA with the existing privacy rules under which we  
16 are operating now. Thank you.

17 MS. GLADSTEIN: Good morning. My name is  
18 Margaret Gladstein. I'm here on behalf of the  
19 California Retailers Association.

20 The CRA values our customers' privacy, but we  
21 do have concerns about the implementation of CCPA. I do  
22 concur with the issues raised by Sarah Boot of the  
23 California Chamber of Commerce, but separately, I would  
24 like to say that the California Retailers Association  
25 seeks clarification of the nondiscrimination section of

1 CCPA section 1798.125.

2 CRA believes that regulations should make it  
3 clear that retailers and others can continue to offer  
4 loyalty and rewards programs, which are very popular  
5 with consumers. 80 percent of Americans belong to at  
6 least one program. We believe the regulations should  
7 clarify that consumers can choose to participate in  
8 loyalty programs that offer incentives such as rewards,  
9 gift cards, or certificates, discounts, or other such  
10 benefits, and businesses may continue to offer them.

11 We also believe that this section needs to be  
12 clarified so that apps that require personal information  
13 to provide the function expected do not run afoul of  
14 CCPA. For example, a retailer's app that allows a  
15 consumer to find the closest store or to place an order  
16 must be able to collect the personal information needed  
17 to function properly. If a consumer downloads the app,  
18 but doesn't provide the needed information, that app's  
19 failure to work should not be considered discrimination.

20 We will be providing written comments and we  
21 look forward to working with your office as  
22 implementation moves forward.

23 MR. KATZ-LACABE: Hi, there. My name is  
24 Mike Katz-Lacabe and I represent Oakland Privacy, a  
25 group of privacy activists in the East Bay.

1           Section 1 of the California Constitution  
2 states, quote, All people are by nature free and  
3 independent and have inalienable rights. Among these  
4 are enjoying and defending life and liberty, acquiring,  
5 possessing property -- and the good part here --  
6 pursuing and obtaining safety, happiness, and privacy.

7           The California Consumer Privacy Act is a good  
8 step towards realizing the right to privacy enshrined in  
9 those words of the California Constitution. It has been  
10 called the California version of the GDPR.

11           As a privacy advocate, I am amused at how many  
12 of the previous speakers claim that their industry or  
13 clients value privacy when they only reluctantly comply  
14 with existing privacy regulations. If those words were  
15 true, hundreds of thousands of people wouldn't have  
16 pushed for this to be placed on the ballot and forced  
17 the legislature to act.

18           Mobile carriers were so concerned about  
19 privacy and consumer trusts that they sold our location  
20 data to third parties.

21           While implementing the law, it is important to  
22 put California citizens first by erring on the side of  
23 transparency and consumer control. So, for example,  
24 when we talk about the uniform opt-out logo, while I  
25 think that's a good idea, I think the preference would

1 be an opt-in logo.

2 We know, studies have shown, that consumers  
3 when faced with a default configuration or a default  
4 choice will leave that and not change it. The uniform  
5 opt-out favors businesses and not the interests of  
6 consumers.

7 In fact, businesses should be required to  
8 disclose what data is collected and why and with whom  
9 the data is shared on its website in a  
10 publicly-accessible way so that consumers, many of them  
11 will never request the information, don't actually need  
12 to request the information, they can just look on the  
13 website. An example of this is the list of third  
14 parties with whom personal information may be shared  
15 that PayPal makes available on its UK website. One  
16 thing is certain, PayPal would not have provided this  
17 information without a requirement to do so.

18 The only way to protect the privacy of  
19 Californians is to ensure that we control our own  
20 information and not businesses. We know that when  
21 companies control the personal information of  
22 Californians, market forces encourage new and innovative  
23 uses of our information and ways to violate our privacy.

24 We know that in the absence of transparency,  
25 businesses will use our personal data in ways that are

1 not only nonobvious, but that may be dangerous to  
2 consumers. Sorry about that.

3 For example, I touched upon the example of  
4 mobile carriers selling location data of cellular phone  
5 customers to third parties. Those third parties sold it  
6 to others who sold it to others until it was available  
7 for purchase by essentially anyone, including abusive  
8 partners seeking to find their victims.

9 Instead of -- I'm sorry. To be clear, there  
10 is a lot of unnecessary fear-mongering about this law;  
11 and it's very clear that the organizations that say they  
12 value consumers' privacy are more adept at finding ways  
13 to complain about the law than finding solutions to help  
14 enact it and actually protect the privacy of the  
15 consumers that they claim to cherish and value. Thank  
16 you.

17 MR. BROOKMAN: Good afternoon. My name is  
18 Justin Brookman. I'm here today on behalf of Consumer  
19 Reports. We are the largest independent testing lab in  
20 the world. We test thousands of products a year for our  
21 magazine and website and apps on behalf of our 7 million  
22 members. We also engage in privacy and advocacy.  
23 That's the capacity in which I'm here today.

24 Consumer Reports was the first organization to  
25 get behind the ballot initiative that led to the CCPA.



1 We have some disagreements on how it was watered down  
2 somewhat in enactment, but we strongly support the four  
3 core principles behind it: Transparency, tell people  
4 what you're doing; access, give people access to their  
5 information; the right to delete data that's not needed  
6 anymore; and the opt out of the sale of their  
7 information to third parties.

8 We think these should be fairly  
9 noncontroversial, but we are concerned we have heard a  
10 lot of efforts from this room to shrink the scope of the  
11 CCPA beyond what was intended by the private drafters.  
12 We have heard a lot of people asking for limiting the  
13 categories of personal information and identifiers  
14 beyond what was intended. I think it's quite clear from  
15 those definitions and the definition of sale that CCPA  
16 was designed to address on-line and cross-app tracking,  
17 even if that data wasn't tied to an off-line identifier,  
18 it was just tied to a cookie or mobile identifier.

19 I strongly disagree with the suggestion that  
20 several folks have said that CCPA mandates full-tie  
21 pseudonymous data to off-line identifiers. But if that  
22 needs to be clarified through regulations, I don't think  
23 you will hear a solitary privacy advocate disagree with  
24 that.

25 More of your processed information for

1 on-line advertising --

2 (Interruption by the Reporter.)

3 THE HEARING OFFICER: Slow down.

4 MR. BROOKMAN: I might want to slow down.

5 It's other cross-site, cross-app, cross-device data,  
6 whether it's for measurement or through social widgets,  
7 it's important to clarify the CCPA's protections apply  
8 to those.

9 Also, the Attorney General should also  
10 consider mechanisms to make sure that choices are  
11 scalable and persistent. It's not really practical for  
12 consumers to opt out every single website they go to or  
13 every single store they visit. We need to find ways to  
14 globally opt people out of data sale.

15 As you heard from one of the previous  
16 speakers, industry opt-outs today are actually quite  
17 difficult to use. There has been a lot of reference to  
18 the Digital Advertising Alliance opt-out solution.  
19 Unfortunately, that solution has a lot of problems. It  
20 isn't universal. It doesn't fundamentally address the  
21 data sale and sharing issue. The technology behind it  
22 is actually quite broken. We would be extremely leery  
23 about a compliance solution that just repurposed this  
24 existing and flawed model.

25 As a previous speaker said, this is the reason

1 the CCPA was enacted, because existing self-regulatory  
2 programs haven't been sufficient. We need to look to  
3 other mechanisms: persistent signals, potentially  
4 centralized databases of identifiers. Senator Wyden has  
5 proposed legislation at the federal level to try to  
6 think through what a universal opt-out solution might  
7 look to. I think some of those ideas can be useful for  
8 many regulations.

9 I want to talk briefly about the privacy on  
10 shared devices, and households has come up today a few  
11 times. Some in the industry have been asking for pretty  
12 broad exemptions to this concern. I think the concern  
13 is legitimate. If I live in a shared group home, I  
14 shouldn't be able to go to my ISP and find out what  
15 every single person in my household is doing. I'm  
16 sympathetic.

17 I don't think the solution though is to  
18 exclude device and household data entirely from the  
19 bill. Some of the protections, I think, certainly  
20 should still apply. Transparency should tell people  
21 what's going on. The opt-out rights should still apply.  
22 Contrary to what some folks have suggested, the opt-outs  
23 are not subject to authentication, and I think those  
24 need to apply to the device and household level.

25 I think some limitations around access may be

1 reasonable for these environments, but I don't think  
2 that taking these categories out entirely is a good  
3 idea.

4 A couple more quick things, not too quick  
5 though.

6 Transparency, the AG directed to provide that  
7 privacy notices are readable. I think this is a fair  
8 concern. I want to caution against making privacy  
9 notices overly simplified and too high-level such that  
10 they don't convey a lot of meaningful information.

11 Privacy policies are fundamentally most useful  
12 for folks like you-all: regulators, for the press, for  
13 testing organizations like Consumer Reports. We  
14 evaluate products today based on looking at their  
15 privacy policies for giving them scores on privacy and  
16 security to get a sense of what they do. It's actually  
17 not that easy, because privacy policies tend to be vague  
18 and inscrutable today. I think CCPA's transparency  
19 provisions tend to help with that, but perhaps  
20 regulations specifying need to be clear about certain  
21 elements like methods for collection, security  
22 protocols, de-identification methods would make my job  
23 easier and I think it would help introduce external  
24 accountability.

25 Finally, on the discrimination and

1 pay-for-privacy, this is one of the more controversial  
2 elements of the bill, certainly, from the privacy  
3 advocate community. This is something that was  
4 dramatically different from ballot initiative. We are  
5 generally skeptical about pay-for-privacy provisions,  
6 but in an era of increasing corporate concentration  
7 where consumers have fewer and fewer choices, we are  
8 especially concerned that, in those environments,  
9 there's not a lot of alternatives. So some degree of  
10 guidance that -- where industries -- where there are  
11 fewer consumer choices, some indication that  
12 discriminatory programs to make people pay for their  
13 privacy are more likely to be considered coercive or  
14 unreasonable, I think, would be appropriate. Thank you  
15 very much.

16 MR. MASSAR: Hello. My name is J.P. Massar  
17 with Oakland Privacy in the Bay Area. We are a group  
18 concerned with individual and consumer privacy,  
19 surveillance regulation, and government transparency.

20 As the last speaker touched upon last, I would  
21 like to address the privacy considerations, especially  
22 with respect to the clause of the new law that says  
23 businesses may charge if things are reasonably related  
24 to the value to the consumer by the consumer's data.

25 I have read that clause about ten times now.

1 I have no idea what it means. I doubt if anyone in this  
2 room has any good idea what it means.

3 But one thing does seem clear, it seems to  
4 provide the opportunity for businesses to create a  
5 privacy tax, especially on the millions of  
6 below-poverty-level and low-wage individuals and  
7 households in California. And that's not good.

8 On-line services are all but essential in the  
9 21st century. You know, the FCC may be trying to limit  
10 access and going in the other direction, but that's not  
11 the way California should be going. Many people need or  
12 are required access to services and to on-line utilities  
13 they have come to -- they have come to expect. You  
14 know, phone access, phone access is considered essential  
15 and provided by law by telcos to low-income households.

16 I think the Attorney General must ensure that  
17 people are not nicked and dined to death; they're not  
18 priced out of access to on-line services without being  
19 forced to surrender their privacy. Otherwise, the  
20 California right that others have alluded to in the  
21 constitution will -- and that this law is intended to  
22 empower -- will become meaningless.

23 Finally, I think, as another colleague  
24 mentioned in a previous hearing, there is an important  
25 distinction between businesses that are selling products

1 and businesses that -- where the consumer, in effect, is  
2 the product, right? And absolutely businesses that are  
3 selling products should not be allowed to impose any  
4 kind of privacy tax. The privacy tax needs to be zero  
5 when dealing with businesses who are selling shirts and  
6 refrigerators on-line. Absolutely.

7 And just to reemphasize, for other businesses  
8 who are providing these services, again, you cannot  
9 allow millions of California residents and households to  
10 be basically priced out of these services by being  
11 nicked and dimed over 10, 20 different services all  
12 charging fees. So thank you very much.

13 MR. JOHNSON: Hi. I'm Brett Johnson with the  
14 California Life Sciences Association, and we are an  
15 association representing both large and small medical  
16 device, bio-pharmaceutical companies, as well as  
17 academic and research institutions, and a number of  
18 service providers, including law firms, venture capital,  
19 and others servicing the life sciences industry here in  
20 California.

21 I'll be brief. We essentially really had  
22 three main issues that we wanted to comment on. The  
23 first two which would be the definition of "consumer"  
24 and the definition of "sale." I think a lot of our  
25 comments have been pretty well covered by Sarah Boot of

1 the Chamber and Pete Isberg of the American Payroll  
2 Association.

3 But to run through those quickly, first,  
4 regarding the definition of consumer, we believe there  
5 may be some problems in application, at least for our  
6 industry. Primarily, we would like some clarification  
7 as to how it applies to employees. I believe a lot of  
8 that has already been covered today.

9 However, we are also concerned as to its  
10 application in business-to-business contacts or  
11 affiliate-to-affiliate contacts. For instance, in this  
12 regard, does the information of principal investigators  
13 and clinical site staff in regards to any sort of  
14 research conducted for our members, how do those fall  
15 under the scope of the CCPA.

16 Second, on the definition of sale, we have  
17 questions as to how it applies to transfers or sharing  
18 of information for, quote unquote, other valuable  
19 consideration. How does this comport with consumers'  
20 reasonable expectation of the meaning of the word  
21 "sale."

22 And, furthermore, and most importantly for our  
23 members, how does this definition apply within the  
24 context of intracompany or affiliate-to-affiliate  
25 transfers of value, particularly if we consider much of



1 this information as having value.

2 And our third point, which is one that's of  
3 particular concern to the life sciences industry here in  
4 California, as well as others in healthcare, even though  
5 we had Senate Bill 1121 last year, which did provide  
6 some additional clarification on exclusion, there are  
7 still concerns as to the extent to which HIPAA, the  
8 HIPAA de-identification standard, will be deemed  
9 sufficient to meet the CCPA's definition of  
10 de-identified. And this would come in in situations  
11 where one of the entities with which we must work to  
12 either monitor medication or a device once it's on the  
13 market. If our affiliates are receiving information  
14 that has already been de-identified under the HIPAA  
15 standard, it will be very difficult for us to afford  
16 individuals' rights on data that has already been  
17 de-identified or for us to further de-identify data up  
18 to the standard of the CCPA if we had already received  
19 it as de-identified.

20 So, again, we are hoping that there is some  
21 clarification and that our members are not having to  
22 deal with the confusing set of obligations between the  
23 CCPA and HIPAA.

24 And that's HIPAA, H-I-P-A-A -- not  
25 H-I-P-P-A -- which for those of us in the industry know

1 how frustrating that can be.

2 And then I'll just make two other quick notes.  
3 I know that the GDPR has been mentioned today, but we do  
4 ask, because so many of our members do have to deal in  
5 the EU, that where there are administrative  
6 requirements, forms, or things of that nature, that we  
7 do look to align to the GDPR where possible.

8 And then just one other final note, because  
9 one of our members raised it, just asking for  
10 clarification on whether or the extent to which  
11 do-not-sell requests have to comply with the, quote  
12 unquote, verifiable consumer request obligations in  
13 other areas of CCPA.

14 So thank you for the opportunity to comment  
15 and look forward to working with you going forward.  
16 Thank you.

17 MR. BARBARA: Thank you for your time today.  
18 We have had some great comments and I would like to  
19 build on them by talking a little bit about compliance  
20 time lines.

21 My name is John Barbara (ph), and I'm a  
22 certified information privacy professional. I have been  
23 extremely fortunate -- or extremely fortunate that, over  
24 the course of my career, I've worked for many companies  
25 in several different industries, and it's allowed me to

1 develop a unique perspective on privacy as well as  
2 understanding the technical challenges around  
3 operationalizing privacy controls.

4 As a consumer, I strongly support the  
5 underlying goals of the CCPA. Privacy is a fundamental  
6 social value, one to which I have dedicated my  
7 professional career, as recognized ambiguity in the law  
8 has raised concerns, but uncertainty as to when changes  
9 must be implemented is also a major issue.

10 As you work through the issues, I ask the AG  
11 to consider that the act appears to become operative  
12 before companies have had a reasonable amount of time to  
13 implement measures required by the regulations. As  
14 written, companies are given six months or less to  
15 implement requirements of unknown complexity with no  
16 consideration for the level of effort required by the  
17 average small- to mid-sized company.

18 Now, proponents of the CCPA often cite GDPR as  
19 an example of why they believe the requirements of the  
20 new California law are easily obtainable. This may be  
21 true for large, international companies, however, the  
22 CCPA will apply to many small- and mid-sized U.S.-only  
23 businesses to which the GDPR has never applied.

24 Additionally, the GDPR was an update of  
25 existing law, the EU directive, so affected companies

1 were already in near-compliance with the new GDPR  
2 requirements.

3 Unlike the GDPR, the CCPA will require many  
4 small- and mid-sized U.S.-only businesses to build  
5 entirely new programs from the ground up.

6 Furthermore, companies were given two years to  
7 implement measures required under the GDPR. The time  
8 line for implementation of the GDPR and the EU directive  
9 spanned nearly six years from initial proposal to the  
10 ultimate implementation date. Drafters took into  
11 account the complexities of the requirements and gave  
12 companies several years to build systems to meet those  
13 requirements.

14 Again, depending on the complexity of the  
15 measures identified in the AG rulemaking, it may take  
16 more than the allotted six months to design, develop,  
17 purchase, test, secure, and ultimately implement systems  
18 that meet CCPA requirements.

19 For example, just for one piece of the  
20 reporting requirement, to make sure we have logs on hand  
21 for the data that we collected and used in the past  
22 year, I asked about using existing system logs.  
23 Conversation went like, IT, "Yeah, well, you know, we  
24 keep it for 30 days."

25 "Okay. Can we just change it to a year?"

1 "Yeah, no. We'll need to write new code to  
2 log the data that you want. That will make the logs  
3 bigger and there is not permanently enough space in the  
4 system, so we'll need to redesign the architecture. Oh,  
5 and if you are going to want to add personal information  
6 to those logs, we need to redesign the security. And if  
7 you want to keep a year's worth of data, well, then  
8 we're going to need to buy new servers to have enough  
9 space. That means finding rack space in our data  
10 centers, building, configuring new network --"

11 (Interruption by the Reporter.)

12 MR. BARBARA: That's what it's like when IT  
13 talks to you.

14 But then, "Okay, let's just put it in the  
15 cloud."

16 Well, you are still going to need to purchase  
17 that service and you need to make sure it's secure. So,  
18 again, you are going to have to get purchasing involved,  
19 you have to go to -- you've got legal to negotiate the  
20 contracts, and that's all in addition to our day jobs.  
21 And so that's just for one part of one CCPA requirement.

22 So I'm here today to ask that each rule  
23 specifies its own time line for compliance. Now, this  
24 is an approach that has been taken by U.S. federal  
25 regulatory agencies in the past. For example, the SEC's

1 robocall rules specify different time frames for  
2 compliance with different measures. It gave companies  
3 nine months to implement the abandoned call rules, 11  
4 months to implement an automated interactive opt-out,  
5 and 18 months to implement and obtain prior express  
6 written consent.

7 Now, I'm committed to meeting the requirements  
8 of the CCPA, however, specifying six months to comply  
9 with the regulation, absent any knowledge of the  
10 complexity of the requirements, seems arbitrary and  
11 almost capricious. Therefore, I respectfully submit  
12 that compliance time frames should be specified by the  
13 AG in each rulemaking based on the demands of the  
14 specific rule that gives companies a reasonable period  
15 of time to meet the requirements of that rule.

16 I'm going to give it my best shot, but please  
17 give me enough time to get it done. Thank you for your  
18 time today.

19 THE HEARING OFFICER: So this is the awkward  
20 part of the forum where we are going to be waiting  
21 patiently and give as many speakers what I refer to as  
22 air courage, need to come down and provide additional  
23 comments. So we are going to sit up here and just look  
24 out at an indistinct point somewhere and just be patient  
25 and wait for speakers who might want the opportunity to

1 come down and provide comments that just need a little  
2 bit of extra time to get down here.

3 UNIDENTIFIED SPEAKER: Hi. Since there is  
4 time, I was here for the California Department of  
5 Education, and I just would love to put in there that  
6 I'm getting a lot of calls from folks asking how this is  
7 going to impact schools and how it interplays with other  
8 laws that have been mentioned, like FERPA and the  
9 Student On-Line Personal Information Protection Act. So  
10 any guidance on what this means for schools would be  
11 greatly appreciated.

12 MR. USI: Good afternoon. George Usi, I am  
13 the chairman of the California IPv6 Task Force for a  
14 scientific research organization advocating Internet  
15 upgrade and use of latest security technologies, et  
16 cetera.

17 We know that, within the law, there was a  
18 statement for tracking of IP address, but we want to be  
19 sure that, in consideration of the rulemaking for IP  
20 address tracking, that you are specifically stating  
21 whether it is IPv4, IPv6, and the different variations  
22 and technicalities within IP addressing, and that you're  
23 specific so controls and measures can be addressed  
24 properly.

25 You can work with Aaron or the Task Force in

1 regards to that. We look forward to working with you on  
2 that matter if you need that definition. Thank you.

3 THE HEARING OFFICER: Thank you, everybody,  
4 for coming. At this point, we are going to close the  
5 formal part of our public comments. We are going to  
6 hang out in the room, so please feel free to speak up,  
7 speak with us, if you would like, or if you have any  
8 questions. We are happy to talk to you a little bit  
9 more about the rulemaking process, and thank you again.

10 (The proceedings adjourned at 12:33 p.m.)  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25

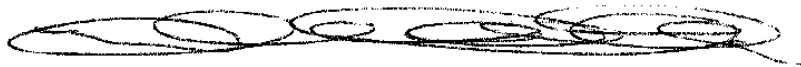


REPORTER'S CERTIFICATION

I, Mandy M. Medina, Certified Shorthand Reporter,  
in and for the State of California, do hereby certify:

That the foregoing was taken before me at the  
time and place herein set forth; that the testimony  
and proceedings were reported stenographically by me  
and later transcribed into typewriting under my  
direction; that the foregoing is a true record of the  
testimony and proceedings taken at that time.

IN WITNESS WHEREOF, I have subscribed my name  
this 14th day of February, 2019.



Mandy M. Medina, CSR No. 11649