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



1	APPEARANCES
2	
3	The Hearing Officer:
4	STACEY SCHESSER, Supervising Deputy Attorney General,
5	State of California, Office of the Attorney General
6	Also Present:
7	LISA B. KIM, Deputy Attorney General, State of California, Office of the Attorney General
8	<del>-</del>
9	DANIEL BERTONI, Staff Services Analyst, State of California, Office of the Attorney General
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	
21	
22	
23	
24	
25	



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.



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

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

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

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

The bathrooms are outside and to the left of



1 | this room.

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

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

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

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

The public hearings that take place during the



formal rulemaking period will be live and webcasted and
videotaped. All written comments and oral comments
received during those public hearings will be available
on-line through our CCPA web page, which is here.
We encourage you to stay informed throughout

We encourage you to stay informed throughout the process by continuing to visit our website at www.oag.ca.gov/privacy/ccpa.

Finally, we are going to walk through some of the areas on which we will be seeking public comment.

CCPA section 1798.185 of the civil code identifies specific rulemaking responsibilities of the AG. The areas are summarized here in 1 through 7. Please keep in mind these areas when providing your comments today.

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

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

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

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

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



1 | right to opt out?

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

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

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

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

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

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

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

Nonprofits, however, are still nevertheless



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

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

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

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

We also rely on commercial data companies to



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

The legislative exemptions, therefore, while wonderfully well-intentioned, can adequately protect us from the costly impact of the CCPA. In fact, we may be the first to suffer the full impact of changes when our commercial partners are forced to give us an ultimatum due to the increased cost of complying with the CCPA:

Pay us more or cease entirely your outreach to

12 percent of the United States population residing in California.

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

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



beneficiaries and the work that we do on their behalf.

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

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

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

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

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



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

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

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

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



1 level of data about that individual.

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

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

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

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

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



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

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

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

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

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

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

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

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



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

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

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

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



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

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

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

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



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

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

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

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

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

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

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

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

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

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

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



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

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

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

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

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

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



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

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

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

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

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

Second, in section 140(y) and other sections



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

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

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

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



1 | consumer, " unquote.

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

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

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

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



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

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

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

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

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

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



10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

- that point out the most glaring concerns and glaring 1 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 be reasonably linkable to an actual person, and clarify 6 7 the right to create de-identified aggregate and 8 pseudonymous information.
  - From the wireless industry standpoint, one of the issues that is particularly concerning is one that you have heard about several times already today, which is bringing the definition of household and devices into the definition of personal information.
  - We urge the AG to provide guidance on verifying consumer requests and what constitutes reasonable efforts to verify and what are acceptable means of verifying consumers.
  - The Attorney General should consider how to authenticate other users on the same account who is not primary -- who are not the primary account holder, as is typically the case for our family plans.
  - The current text can be interpreted to allow a consumer to request an extensive set of personal information about his or her spouse as a member of the household, potentially compromising the privacy and



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

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

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

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



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

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

We request -- we request -- that the

Attorney General provide -- one, provide flexibility for
businesses to verify consumer requests; and two, provide
increased transparency to consumers.

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

In cases where a third party intends to make a



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

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

The CCPA removes basic, needed, nonsensitive data from the marketplace that we rely upon and creates competitive disadvantages for California businesses.

Small businesses rely upon consumer data to improve products and services and to find new customers and business partners.

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

1 legal fees and technology costs.

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

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

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

MR. ISBERG: Good morning. My name is

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

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

Payroll Association, which is a nonprofit association

7 | representing over 20,000 payroll professionals across

8 | the United States.

3

6

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

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

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

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

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



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

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

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

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

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



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

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

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

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



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

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

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

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



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

MR. ELLMAN: Good morning. My name is

Eric Ellman. I'm the Senior Vice President of Public

Policy and Legal Affairs for the Consumer Data Industry

Association, CDIA.

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

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

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

First, I want to address fraud prevention



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

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

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

Second, third party notice requirements:

Section 1798.115(d) of the act prohibits third parties

from selling personal information about a consumer that



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

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

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

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



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

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

We request clarity that inferences drawn from any personal information to create a consumer profile is not personal information when the personal information upon which the inference is to be drawn have been de-identified and de-aggregated. Those are, again, 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 of a number of federal and state laws: 4 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 Safequards 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. 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

inconsistencies and problems, which ultimately will have



25

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

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

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

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

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

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



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

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

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

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



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

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

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

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

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



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

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

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

MS. SMITH: Good morning. My name is

Heather Smith and I'm the president of the American

Advertising Federation, Sacramento Chapter here, as well

as the lieutenant governor for District 14, which

comprises all of Northern California and Reno.

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



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

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

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

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



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

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

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

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

Consumers have enthusiastically embraced the



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

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

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

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

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



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

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

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

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

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

The DAA will release guidance on the application of the principles of transparency and accountability to public advertising.

The main avenue through which consumers receive disclosures and choices is through the DAA YourAdChoices icon, which is served in or near ads over a trillion times per month worldwide. The YourAdChoices icon provides transparency outside of the privacy policy, and clicking on it allows consumers to access simple, one-button tools to control future collection and use of data for interest-based advertising.

Consumer awareness and understanding of the program continues to increase; and in 2016, studies showed more than three in five consumers, or 61 percent, recognized and understood what the YourAdChoices icon represents.

What was I at? Pretty close?

We'll go to our recommendations. While we do strongly support the CCPA's intent to give consumers a choice about how the personal data is shared, we're concerned about the negative impact on certain serious sections of the CCPA. I believe the law can be clarified through rulemaking to provide improved consumer protection and guidance to businesses.

Section 1798.115(d) of the CCPA prohibits a



company from selling consumer personal information that it did not receive directly from the consumer unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt out of that sale. We urge the AG to recognize that a written assurance of the CCPA compliance is sufficient and reasonable.

Sections 1798.105 and 1798.120 of the CCPA allow consumers entirely to opt out of the sale of their data or delete their data. The law does not explicitly permit a business to offer consumers the choice to delete or opt out regarding some but not all of their data. We request that the AG clarify that businesses may offer reasonable options to consumers to choose the types of sales that they want to opt out of, the types of data they want deleted, or to completely opt out and not have to just provide an all-or-nothing mention.

And, lastly, section 1798.110(c) of the CCPA requires a business's privacy policy to disclose to a consumer the specific pieces of personal information that the business has collected about the consumer. We ask the AG to clarify the business does not need to create individualized privacy policies for each consumer to comply within the law.

Thank you so much for your time today. We



1 look forward to further comment.

THE HEARING OFFICER: We're going to take a break right now for about 10 to 15 minutes. We realize there are speakers that still would like to get up to the podium, so please come back to sit in the front row after the break is over.

(A break was taken.)

THE HEARING OFFICER: Thank you. We're going to begin again. We have received a request from the court reporter to please slow down. So we have also emboldened her to directly interrupt people that are speaking too quickly or too fast. So if she interrupts you, please slow down. As I said to her, this is California. We are supposed to be more laid back, right? So if we can ease -- she's trying to help us by creating a transcript, which, yes, we will post on the Internet on our website after they become available. There has been many requests from the public, and we will be posting event materials as we receive them.

So, for now, we're going to resume for our public comments. And this has been a very active session so far, and so we're grateful, and we continue to welcome people to offer comments and provide them as well in writing. And we're going to put the website back up at the end and make sure that -- I'm sorry --



the E-mail address back up at the end, as well as the mailing address, so that folks know where to send the comments that they are preparing for us.

Thank you again.

MS. MEHLER: Thank you. My name is

Louise Mehler, spelled M, as in mother, e-h-l-e-r. I

promise not to speak rapidly, because my comments are

not prepared. I am going to stutter.

I don't represent anyone. I am a local resident, been informed of this by the Internet, and since I was available, I thought I would stop by.

After listening to the comments so far, which I understood may be half, I am here largely to say, "Help." I am an educated person, reasonably computer-literate. I have never made it all the way through an opt-out procedure. They splinter, they go here and there, they require you to log into your account. And then you get there, you don't know what the definitions are of what you are opting in or out to.

So we need help. We need it from you. As I have listened to the comments, I have understood that this is a threat to the Internet business model, that it depends on, you know, a thread of information to be sold on, some for advertising. The responses you get to surveys are extremely malleable, as we all know,



depending on how the questions are asked. If consumers really valued the advertising all that much, we would not have such a large market for ad blockers.

The other ways in which information is used, when sold, beyond advertising, are even more problematic. So I don't know if this is exactly the forum to say that, you know, we need a way to revise or back away from the model, you know, the advertising-supported model, but I think, ultimately, that's where this is headed.

But on the way there, as you work to implement this law, consider what people can actually see and understand about what's being collected and how it's used. Because, overall, I think it has been used to our harm, and getting a data dump isn't going to help.

So thank you for the opportunity, and please remember all of us out there who don't know what's going on.

MS. COHEN: Hello. Thank you for the opportunity to comment. My name is Allison Cohen and I'm an attorney at Loeb & Loeb practicing in the area of data privacy and security. We represent many mid- to large-sized companies that interact with California consumers. The brands we represent care very much about respecting the privacy rights of consumers, and my

comments today suggest ways in which the regulations could be clarified or the regulations could clarify the CCPA to help businesses provide their services to California consumers, services which are intended to benefit California consumers while also fully respecting consumers' privacy rights.

First, I would like to suggest that rulemaking clarify the categories of personal information, and I know this has been touched upon. I would like to suggest that the categories of personal information include only those categories that are actually or reasonably related to a particular consumer instead of the CCPA's current breadth which extends to personal information capable of being associated with a particular consumer. Such clarification would prevent collection sharing and deletion of more information than is necessary.

Secondly, I would like to suggest that a regulation to exclude personal information collected be developed to address the employee data, something along the lines of excluding personal information collected in the context of or derived from an employment relationship. Such an exclusion would allow employers and their affiliates to continue to use their employees' personal information as necessary for their business



1 operations.

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

Another area that merits consideration is related to the GLBA section. As written, the act does not apply to personal information collected, sold, processed, or disclosed pursuant to GLBA. Many financial institutions regularly sell portfolios within their businesses, and in doing so, consumer personal information is transferred with the commercial sale of the portfolio. Although the individual transactions that are part of the portfolio are protected by GLBA, the sale of the portfolio itself, such as a credit card portfolio or a delinquent account portfolio, does not appear to technically fall within this exclusion. would be helpful if the regulations excluded from the definition of sale the selling of these types of portfolios and transferring of corresponding personal information to the commercial purchaser.

My next comment is related to the uniform opt-out button. The law currently appears to require an all-or-nothing opt-out schematic. However, both businesses and consumers would benefit if businesses were able to offer opt-out options to their consumers.

The AG has the opportunity to authorize businesses to take a more nuanced approach and offer consumers the option to opt out of some selling or



2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

sharing while allowing other selling or sharing to proceed. Such flexibility would provide consumers greater control of their privacy, while also allowing a consumer to continue to reap benefits offered by the business. For example, a consumer may not want a business to share or sell location data, but the same consumer may very much want the business to share purchase history in order to gain access to product discounts and benefits.

Consider a rulemaking to clearly delineate what constitutes effective verification as well. Businesses do not want to have to collect personal information in order to verify a consumer request. business collects only a unique identifier, it may not relate back to a specific individual. The business may not be capable of associating the identifier with a Where does that leave the business? Does the consumer. business have to collect more personal data in order to verify that the identifier is associated with the consumer making the request? Collecting the additional information for verification purposes would be an anti-privacy practice. A regulation that allows a business to decline consumer requests when the business does not have a way of verifying the consumer without collecting personal information would be most helpful.



Thank you very much for the opportunity to comment today and thank you for taking the time and energy and effort to listen to our concerns and suggestions.

MR. FOULKES: Good morning. My name is

Tom Foulkes. I'm the Vice President of State Government

Affairs for the Entertainment Software Association. ESA

is the U.S. trade association that represents the

business and public affairs needs of the computer and

video game industry -- sorry -- for the companies that

develop and publish video games for personal computers,

video game consoles, and mobile devices.

ESA does plan to provide comprehensive written comments to the Office of the Attorney General related to California Consumer Privacy Act, but today, I hope to briefly highlight those priority issues, including exemptions, to help businesses comply with other laws, clarifications regarding access rights and relationship between data and the provided services.

The CCPA empowers the AG to implement various exceptions to comply with federal and state laws, including those related to intellectual property. We feel that the video game publishers need to be able to limit their disclosures where doing so may reveal insights into sensitive technology, efforts to combat IP

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

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

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

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

Thank you for your time and attention to these



1 | important issues for both consumers and companies alike.

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

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

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

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

1 | than the requirements set forth by CCPA.

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

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

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

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

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

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



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

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

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

We support the guiding principles of



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

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

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

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

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



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

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

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



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

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

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

(Interruption by the Reporter.)

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

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

Part of the process of providing title



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

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

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

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

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

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

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

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



1 | flag it and work with DAs all the time.

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

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

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

MR. HARRISON: Good morning. I am

James Harrison. I'm an attorney at



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

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

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

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

From our perspective, there are three top



priorities for your task in drafting regulations.

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

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

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



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

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

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

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

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

Right now, our utilities do not collect data



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

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

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

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



1 | CCPA section 1798.125.

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

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

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

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



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

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

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

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

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



1 | be an opt-in logo.

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

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

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

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



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

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

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

MR. BROOKMAN: Good afternoon. My name is

Justin Brookman. I'm here today on behalf of Consumer

Reports. We are the largest independent testing lab in
the world. We test thousands of products a year for our
magazine and website and apps on behalf of our 7 million
members. We also engage in privacy and advocacy.

23 | That's the capacity in which I'm here today.

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



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

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

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

More of your processed information for



1 on-line advertising --2 (Interruption by the Reporter.) 3 THE HEARING OFFICER: Slow down. 4 I might want to slow down. MR. BROOKMAN: 5 It's other cross-site, cross-app, cross-device data, whether it's for measurement or through social widgets, 6 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 difficult to use. There has been a lot of reference to 17 18 the Digital Advertising Alliance opt-out solution. 19 Unfortunately, that solution has a lot of problems. Ιt 20 isn't universal. It doesn't fundamentally address the 21 data sale and sharing issue. The technology behind it

As a previous speaker said, this is the reason

is actually quite broken. We would be extremely leery

about a compliance solution that just repurposed this



existing and flawed model.

22

23

24

25

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

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

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

I think some limitations around access may be



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

A couple more quick things, not too quick though.

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

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

Finally, on the discrimination and



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

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

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

I have read that clause about ten times now.



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

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

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

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

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



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

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

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

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



the Chamber and Pete Isberg of the American Payroll
Association.

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

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

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

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



3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

1 this information as having value.

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

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

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



1 | how frustrating that can be.

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

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

So thank you for the opportunity to comment and look forward to working with you going forward.

Thank you.

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

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



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

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

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

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

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



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

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

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

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

For example, just for one piece of the reporting requirement, to make sure we have logs on hand for the data that we collected and used in the past year, I asked about using existing system logs.

Conversation went like, IT, "Yeah, well, you know, we keep it for 30 days."

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



"Yeah, no. We'll need to write new code to 1 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. and if you are going to want to add personal information 5 to those logs, we need to redesign the security. And if 6 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 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. 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

regulatory agencies in the past. For example, the SEC's



25

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

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

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

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

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

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

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

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

You can work with Aaron or the Task Force in



regards to that. We look forward to working with you on that matter if you need that definition. Thank you. THE HEARING OFFICER: Thank you, everybody, for coming. At this point, we are going to close the formal part of our public comments. We are going to hang out in the room, so please feel free to speak up, speak with us, if you would like, or if you have any questions. We are happy to talk to you a little bit more about the rulemaking process, and thank you again. (The proceedings adjourned at 12:33 p.m.) 



1	REPORTER'S CERTIFICATION
2	
3	I, Mandy M. Medina, Certified Shorthand Reporter,
4	in and for the State of California, do hereby certify:
5	
6	That the foregoing was taken before me at the
7	time and place herein set forth; that the testimony
8	and proceedings were reported stenographically by me
9	and later transcribed into typewriting under my
LO	direction; that the foregoing is a true record of the
L1	testimony and proceedings taken at that time.
L2	
L3	IN WITNESS WHEREOF, I have subscribed my name
L4	this 14th day of February, 2019.
L5	
L6	
L7	
L8	
L9	Mandy M. Medina, CSR No. 11649
20	Manay M. Medina, CSR NO. 11049
21	
22	
23	
24	
25	

