PUBLIC MEETING ON THE CALIFORNIA CONSUMER PRIVACY ACTS

January 8, 2019

10:20 a.m.

Milton Marks Convention Center

455 Golden Gate Avenue

San Francisco, California

Joan Theresa Cesano, CSR No. 2590
APPEARANCES OF PANEL

STACEY SCHESSER, SDAG
NICKLAS AKERS, SAAG
Department of Justice
Office of the Attorney General
455 Golden Gate Avenue, Ste. 11000
San Francisco CA 94102
SAN FRANCISCO, CALIFORNIA;

TUESDAY, JANUARY 8, 2019; 10:20 A.M.

MS. SCHESSER: On behalf of the California Department of Justice and Attorney General Xavier Becerra, welcome to the first public forum on the California Consumer Privacy Acts. We are at the beginning of our rule-making process on the CCPA. These forums are part of an informal period where we want to hear from you. There will be future opportunities for members of the public can continue to be heard including once we draft a text of the regulations and enter the formal rule-making process. Today our role is to listen. We are not going to be able to answer any questions or respond to comments. Before we start I'd like to briefly introduce ourselves.

My name is Stacey Schesser, I am the supervising attorney general for the privacy unit here at the AG's office.

MS. KIM: My name is Lisa Kim, I am a Deputy Attorney General in the Privacy Unit as well.

MR. AKERS: Nick Akers, chief of the Office of Consumer Law Section.

MR. MAUNEY: Devin Mauney, I'm a deputy instead attorney general in the Consumer Law Section.

MS. SCHESSER: We will be beginning the program
in just a moment, but we have a process to go over for today's forum.

Each speaker will be allotted five minutes. A member of our staff, Devin, is keeping time and he will hold up a card signaling when the speaker has one minute remaining and when time has expired. Please be respectful of the timekeeper and your fellow speakers here today.

We also have a Court Reporter -- we also have a Court Reporter who will transcribing comments. Please speak slowly and carefully for her as well.

When you registered this morning, if you are a speaker, you should have received a number. People will be called down to the front row, which is reserved for speakers, in factors of ten. Please come up to the microphone. It is requested but not required that you identify yourself when you're offering your public comment. It would helpful if you also have a business card to hand that to the Court Reporter.

We also strongly welcome comments by email or mail and you can see that's the email address and the mailing address for you to provide comments to us.

Lastly, bathrooms are to the right of this room just down this hall, and we also encourage people to stay informed throughout this process by going to our website at www.OAG.CA.gov/privacy/CCPA.
Then quickly before we start, is there any media here present today? Okay. Thank you.

CCPA Section 1798.18.5 of the Civil Code identifies specific rule-making responsibilities of the AG. These areas are summarized here in 1 through 7. Please keep in mind these areas when providing your comments today.

Should there be additional categories -- whoop -- oh the joy of technology, right? Okay. Don't worry, we are going to back to that slide in just a minute. There we go.

So category -- topic area number one, categories of personal information: Should there be additional categories of personal information?

Number two: Should the definition of unique identifies be updated?

Number three: What exceptions should be established to comply with state or Federal law?

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

Number five: What type of uniform opt out logo or button should be developed for consumers about the right to opt out?

Number six: What type of notices and
information should businesses be required to provide
including those related to financial incentive offering.

Number seven: How can consumer or their agents
submit a request for information to a business and how
should a business reasonably verify these requests?

At this time we welcome comments from the
public. For those of you with speaker numbers 1 through
10, please come down to the front row and we can begin
opening up the session for public comment. Thank you very
much.

MR. MAUNEY: Anyone else want to come down? Don't
be shy. All right.

MS. SCHESSER: You can step up to the mic.

MR. PITZGER: Good morning. My name is Bo
Pitzger, I'm an Enterprise security architect for the
University of California, however I want to make it clear
that I am not a spokes person for the UC and I'm speaking
strictly in my personal capacity. That said -- is the
microphone not working?

AUDIENCE: It's not on.

MR. PITZGER: Okay. Is this better? Okay. One
more time for the record. My name is Bo Pitzger, I'm an
Enterprise security architecture for the University of
California Office of the President, however I'm here
strictly in a personal capacity and I am not a
spokesperson for the University. That said, the university
does have as part of its mission statement public service
and so in that spirit I want to offer a few remarks.

First of all, with regards to categories of
personal information I know there's been comments in the
public in regards to limiting the scope of that. I would
strongly discourage that. There's been a lot of work at
the University and indeed elsewhere on data sets and I
want to make it clear the via identification like removing
things like names and addresses does not mean you cannot
uniquely reidentify individuals.

While CCPA does not wholly address the issues of
anonymisation, maintaining this broad category role will
makes it a little bit more difficult for physical attacks.

Second, there are various -- excuse me one moment
-- there's various provisions in here that require
consumers to give up their rights or not require,
encourage them by allowing arbitrary charges if they do
not give up their personal information. I think that is a
notion that will lead to obvious abuse, I think that
paying a thousand dollars for Facebook access unless
you're allow them to abuse your personal information.

Next, it was not clear to my reading whether in
fact paper records and non electronic forms of information
were covered by CCPA. I would hope that if there is any
ambiguity in this regard that would be clarified and that public -- paper records would be included. The example being, for instance, the company adequate protects its email but then it gets printed out and is left in a public area. This has been an issue with HIPAA for quite some time and I suspect we will see similar issues here as well.

And I would also note there needs -- there is an implicit standard of care in this and I will add a quick caveat to the lawyers in the room and I'm not a lawyer, so I let you guys define that.

But a standard of care for compliance should include explicit references to the AG-defined use of national standards such as NIST (ph), cyber security framework, which is the basis for FISMA and other Federal regulations, as well as industry best practices. Without that there is no way to measure whether the compliances efforts were adequate prior to an occurrence of a breach.

So I would encourage the AGSU to have done in other areas to periodically publish an update what you would deem to be the minimum compliance, design requirements.

I'd also note, by the way, the University of California at the Berkeley Center For Law and Technology has a lot of resources in this respect and I would suggest
that you might want to talk to Paul Schwartz or Diedre Mulligan or some of the others over there who are internationally recognized experts in this regard.

I might add that, too, we -- we will find that some of these standards are very explicit about what constitutes PI and its handling and I would think that we need to be more inclusive in this regard.

Thank you very much for hearing me out.

SPEAKER (seated): So I'm actually speaker number two but the person to my right is representing an organization that we're a part of, so I'm thinking it might make sense for her to speak first, then if there is anything for me to add I would speak out at that time.

MS. KARASIK: Good morning. Thank you for the opportunity to provide info regarding the implementation of the CPA. My name is Julie Karasik and I'm a resident of San Francisco, California, and I am the Technologist for the Network Advertising Initiative or the NAI.

The NAI is a non-profit the leading self regulatory organization for responsible data collection and use for interest-based advertising.

(Court Reporter speaks; off the record)

MS. KARASIK:

Q I will channel my inner rock star.

Our members include a wide range of technology
business that form the back bone of the digital advertising ecosystem.

The NAI Code of Conduct which is rooted in the Fair Information Privacy Principles requires the NAI members to meet high standards for data collection use including transparency, consumer control and data minimization.

The NAI supports many of the underlying goals of the CCPA in particular giving consumers a choice about how data are to be used consistent with CCPA's requirement for an opt-out choice, the NAI has for years maintained an industry wide opt-out choice that empowers consumers to opt out of interest-based advertising. However, we are concerned that the CCPA suffers from ambiguities that are likely to have profound unintended consequences for both consumers and the robust digital economy.

Therefore, the Attorney General plays a critical role in rule-making in this law. In doing so we urge the AG to consider the following key concerns:

First, the definition of a sale of personal information is ambiguous and it should be clarified that in most cases it does not apply to the process of serving interest-based advertising.

The law's definition contains an exception for business purposes including advertising, but its
application to the programmatic ecosystem is unclear and
contradictory. In most cases these ad buys are not
transactions, but rather auctions of advertising space on
web pages or apps where data is not sold from one entity
to another.

The NAI urges the Attorney General to clarify
that a third party providing a targeted ad to a consumer
on behalf of the business does not fall under the
definition of sales.

Second, complying with individual control rights
could create substantial challenges for education within
the third party advertising industry which seeks to
collect as little personal information as possible.

We agree individuals should have the ability to
exercise control over use of their personal information
and that businesses should strive to provide reasonable
consumer access to this data.

These principles have long been at the core of
the NAI's code which incentivizes companies to avoid
collecting information that identifies the individual
person. But this approach presents challenges with respect
to authenticating individuals for purposes of providing
control such as access, correction and deletion. It would
be an unfortunate outcome if the CCPA is implemented in a
way where companies that attempt to limit their collection
of non personal information are actually required to also obtain identifying data in order to authenticate a user. Therefore, we urge you, the Attorney General, to clarify application of these rules for businesses that do not collect sufficient data to verify the identity of California residents.

Third, it is imperative that the CCPA allow public and service providers to charge a reasonable fee as an alternative to using the current free advertising model. Digital advertising allows companies to provide free or low cost services to consumers.

The CCPA states that the business may offer a different price, rate, level or quality of service to an opted-out consumer, but only when the business meets an ambiguous set of requirements. To remain economically viable, online publishers and service providers must be able to charge a reasonable rate as an alternative to offering ad-support content.

As such, we urge the AG to clarify a company can always charge reasonable rates as an alternative to providing opt out services.

Fourth, the CCPA's requirements for companies to maintain a "do not sell my data" button on their website is ambiguous, potentially requiring companies to add a button to every web page that a company maintains would be
redundant and create a poor user experience, especially on mobile platforms. We ask that the AG specify that the homepage would be sufficient.

Again, thank you for the opportunity to provide input. The NAI looks forward to submitting detailed, written comments and working with you as you develop implementing regulations for this important law. Thank you.

MR. ROSLER: That was a good decision to be able to go quicker. I'm Dan Rosler, I work with a company Flash Talking which is an ad serving technology company. We have offices around the world although I'm based in California.

As Julie mentioned so we are a member of NAI and as a member of that organization we are purposed built around consumer privacy. Our platform does not collect any personal identifiable information in any way. We don't trade that information or anything with third parties.

So in the contents of the CCPA it seems important to us that if companies are taking the approach of emphasizing user privacy and trying to avoid any personal identifiable information in any way, then there should be exceptions for the fact the only information that they would have on the user would be a random user ID, a
character strain that in and of itself doesn't reflect anything about that particular person, and none of the information that can be used to identify that person.

To give you some context of examples where this approach in GDPR has created unexpected consequences as Julie noted, we have been receiving in our European counterparts lots of personal identifiable information from people, driver's licenses, names, addresses, phone numbers, emails, all of this information as those consumers try to identify themselves to us, and so now we are the unfortunate position of receiving, although not through our platform or systems, just receiving email and other methods of personal information that we never intended to have in any way, and that creates a lot of challenges for us or constituents.

So in the context of CCPA it would seem there should be a reward or a benefit to organizations like other members of the NAI who are making efforts to avoid any personal identifiable information in their business and being -- attempting to provide consumers access to this information which does not identify them in any way does cause that burden.

Another note with respect to GDPR which defines IP address as personal information without getting into technical specifics, the use of IP address as personal
identifying information or personal information, I guess, is the definition from GDPR is problematic to the extent IP addresses do not actually individually identify somebody.

Within, for example, a company that may have a single IP address which is being translated out to many users within the company, there is no way of knowing if that IP address attaches to a particular person.

Also IP addresses change over time, therefore a given person may have different IP addresses throughout the day, for some reason, they're renewing or refreshing these IP addresses. So we would encourage CCPA to recognize whether that IP address is not actually personal information to the extent the way the Internet works today. It cannot be attached to a person either uniquely or over time. Thank you very much.

MR. MAUNEY: Speakers with cards 11 through 20, you're welcome to come down to the front row here and again, if you just now decided you'd like to speak, you can come over to the table and pick up a number for later.

MR. SNELL: Good morning. Thanks. My name is Jim Snell, I'm a partner in the data security and privacy group of Perkins Coie in Palo Alto, California. I've been practicing in this area in the privacy law area for 20 years. I'm speaking on behalf of myself and a number of
clients whom we have been working with on the statute and
just wanted to address a couple of points. We will
provide more written comments which we're working on but I
thought it was important to come here today and just
mention a few things.

I won't repeat what the spokesperson from NAI
already said other than to say we agree with everything
that's been said by the NAI with respect to those
challenges.

With respect to the rule-making, I just want to
touch on four points briefly. First, the importance of
establishing safe harbors for businesses. The CCPA
imposes obligations on businesses, but in many respects
lacks detail about how those obligations are to be
fulfilled and the Attorney General can and should
establish procedures that businesses could follow and safe
harbors related to those procedures so that businesses
could follow established procedures and honor obligations
in ways that do provide safe harbors for their conduct and
insulate claims from complying with AG recommended and
endorsed proceedings.

Second, the non discrimination provisions of the
CCPA as currently drafted and contain confusing and
conflicting exemptions in our view. He would appreciate
some clarification and guidance on interpreting those
sections, in particular in building on what prior speakers have said, allowing businesses to provide a different level quality and service to users who exercise their opt-out rights, particularly where data -- if data that's being disabled is needed to provide the original service as necessary, more generally to fund the underlying service. Unless there is clarification we fear that innovation is going to be stifled and that businesses that use as their only source of revenue things, for example, like advertising, are able to survive by charging a reasonable fee for those who want to opt-out.

Third, clarifying the obligations with respect to personal information. There's been some suggestion that the definition of PI is so broad it can be argued to require businesses to link data not already linked to an individual. That's problematic. It's anti privacy, it's anti -- it's not in the consumers' interest to require a business to link information that's not already linked to that individual.

A good example from a prior speaker is IP addresses, which an IP address can be shared within a household, there can be an IP address with respect to Starbucks. If the CCPA were to be interpreted to require businesses to ferret out and link personal information to individuals in order to fulfil their obligations that
would not be in the interest of consumer privacy, it would be an increasable burden on businesses.

And last, aligning the CCPA more closely with existing regimes. An example that's been given by some is the GDPR companies that have invested a lot of money in GDPR compliance. The CCPA has some similarity to the GDPR but the obligations differ, and aligning the CCPA with the GDPR and other regimes, other privacy regimes of businesses have already invested in complying with, would be in consumers' interest and businesses' interest, and it's a common sense way to address those who have already been compliant with other regimes.

And actually my first comment on safe harbors, was providing safe harbor, for example, for businesses that are GDPR compliant would be in everybody's interests. And with that, I'll rest. Thank you for your time.

MS. BUO: Good morning. Good morning. My name is Vera Buo and I'm here on behalf of the California Chamber of Commerce. Our goal for the AG rule-making process is to make sure the CCPA is workable for all businesses and to address unintended consequences of hastily passed law, many of which run counter to its privacy goals.

Our first request for the AG's office is to keep in mind throughout this process that in addition to data brokers and very large companies CCPA applies to the
incredibly broad category of businesses in almost every industry and that's any business that annually receives the personal information of 50,000 more consumers households or devices. It may sound like a high number at first but it's not given CCPA has a very broad definition of personal information which has been discussed, includes IP addresses and so very much more.

For example, CCPA applies to businesses of 50,000 visitors to their website per year. You divide 50,000 by 365 days in a year and if you have on average 137 online visitors are going to meet the threshold. And so you think of all the businesses, many small businesses like convenience stores or restaurants that conduct an average of 137 transactions in a day, it is going to be challenging for them to comply with this law especially as it's currently written.

The Cal Chamber, in addition to a number of other industries, are working together to draft comprehensive written comments with specific proposed language for your consideration for regulations. We intend to submit that by the end of month. There are a lot of problems with CCPA, some of which can and should be developed with the role of making progress. As for today we will provide one example, a significant example.

The CCPA requires businesses to provide consumers
with specific pieces of information the business has
collected after receiving a verifiable consumer request
and yet the CCPA does not define what specific pieces of
information means. It could mean that businesses must
transmit incredibly sensitive information like credit card
numbers or birth dates back to a consumer, which creates a
risk of inadvertent disclosure to a fraudster posing as
the consumer making mistakes for verifying consumer
requests incredibly high.

Additionally, in an effort we believe to
encourage privacy protected practices CCAP states the
business is not required to relink or reidentify data, yet
a business can not provide specific pieces of information
back to the consumer without relinking or reidentifying
data in order to match it to the person making the
request.

It's a glaring inconsistency in the law as
written and it should be clarified. And all of this runs
counter to common sense principles of privacy. Ultimately
we know that the AG office's goal in the process is to
protect consumers and we have that same goal. We look
forward to working with your office throughout this
process to meet it. Thank you.

MS. GLADSTEIN: Good morning. My name is
Margaret Gladstein and I'm here on behalf of California
Retailers Association. CRA represents all segments of the retail industry including restaurants, grocery and other mass merchandise retailers.

We have -- we appreciate the importance of CCPA and our members are already working on complying with that law. We concur with the previous comments especially the representative from Perkins Coie who spoke about the importance of a safe harbor and the comments just made by Ms. Buo of the Chamber. But our particular concern today will also be submitting written comments has to do with the important of loyalty programs and their continuing existence.

80% of all Americans belong to some sort of loyalty program through a retailer or other type of organization. These are very popular with consumers. We believe it is the intent of the law based on the testimony that was presented during the hearings of the legislature that these programs be able to comment to exist, but as previous speakers have stated there is some clarification needed around these programs that they will be able to continue to exist and retailers who offer them, much the same way they do today and consumers can continue to enjoy them in some of the same way they do today.

So we will leave, again submitting specific comments, but I wanted to raise these issues today and
look forward to working with you as we move forward in this process.

MR. MAUNEY: Ready for the next group, those that are numbers 21 through 30, please come down to the front row here.

MS. FELICIA: Thank you for hearing from the public today. My name is Elizabeth Felicia and I'm vice president of policy at Common Sense. We are a national advocacy organization representing parents, kids and educators. We're dedicated to improving outcomes and equity for kids and families. Increasingly that means ensuring they are protected online and that their identities and private information are treated responsibly.

As co-sponsors of the CCPA we believe many of the expressed concerns about the bill can and will be resolved in this rule-making process. The Attorney General will establish the rules of the road for this historic law, we appreciate the time and effort this office is taking to fulfill its essential role.

Since we're all here today to hear from the public let's remember what the public has voiced time again, that they are concerned about their privacy online. We asked parents and teens in a national survey last year and nearly all teens, 87% and parents, 93% feel it's
important for sites to ask permission before selling or sharing their personal information and more than 90% said it's important that sites clearly label data they collect and how it will be used. This law responds directly to consumer demands and the AG's office will help ensure meaningful, robust set of protections for kids and all consumers.

There is more work to be done in legislature, we need to expand it to strengthen protection such as minimizing overuse of consumer data and we need to guarantee departments like yours have resources that you need. That's for another day. So today we thank you for hearing from the public and for your leadership.

MR. MEDIATE: Hello. My name is Trevor Mediate and I'm a data privacy consultant with Grant Thornton. Today I speak in a personal capacity and not representing the company.

Regarding the right to access, consumer's are permitted to receive a copy of personal information businesses collected and are maintaining on them. However, an existing point of ambiguity and contention under the similar law as the GDPR, is whether inferences businesses collect based on personal information must be shared with the consumer. Businesses have a vested interest in collecting inferences on consumers to improve and inform
their own services, to better target advertising, and to enrich data sets sold to or shared with other organizations.

However, the prescriptive nature of these inferences arguably make their use more consequential to consumers than directly identifiable personal information. As they reveal unparalleled insights into how consumers make decisions and present opportunities to exploit those insights according to the unknown goals of any party with the competence to do so, expressly recognizing and addressing the disclosure of the inferences derived from personal information resolved several issues regarding the definition of personal information.

Increasingly, businesses are collecting what is traditionally considered non personal information to recognize and track individual devices with full knowledge that a deep understanding of consumers' Internet connected device reveals equally deep knowledge about the consumer who owns them.

We hear often that business organizations want to avoid compliance challenges that come with collecting personal information, but simultaneously, desire the benefit that targeted marketing and more opaque data management practices bring.

What I ask is that the definition of personal
information within the CCPA expressly culls out not only information related to an individual but also any conclusions that are drawn from that collective information and that that information is accessible and able to be shared with consumers in a format which they may understand, under existing data reportable requirements in the CCPA.

I feel giving consumers this information and understanding how businesses see them as a consumer that makes decisions, can help offset the impact of influence campaigns, can empower consumers to make their own decisions, and make the practice of data privacy more tangible and allow consumers to take ownership over that aspect of their lives that is increasingly consequential in 2019 and in every year to come. Thank you.

MR. CARLSON: My name is Steve Carlson, I represent CTIA which is the wireless industry trade association of device manufacturers, carriers and the like. We associate ourselves with some of the earlier comments concerning the need for a safe harbor, the difficulty and dangers of requiring specific pieces of information as opposed to categories of information which is the -- which is protocol in other areas of our state law, but as the wireless industry of particular concern is the definition of information concerning household device
and family. Because relatively uniquely, but not only, there are usually many account holders under the primary account in the wireless industry, and if you cannot link a particular individual with a particular set of data, you are at great risk. I think we have cyber security risks which are overwhelming and really need to be considered, as well as other non attended consequences which we will explore later in our comments.

So we would urge the Attorney General to look at these things. We want this to be workable. We want this to be privacy, but smart privacy. Thank you.

MS. ROSENBERG: Good morning. My name is Tracy Rosenberg and I'm with Media Alliance. We are the Northern California Democratic communications advocate. I hear a large number of people speaking on behalf of the business community and I want to make it clear I'm here to speak on behalf of consumers, specifically lower income and marginalized communities, whose needs need to be considered in this law. I specifically want to address some of the non discrimination clauses in CCPA.

As we talked about, they are a little confusing at best, we don't know what the value of the data to a consumer or to a business actually is and there is some clarification of the language that you're going to have to do, but the existing language regarding disadvantageous
pricing and these relate to the value of data. I'm not insensitive to the needs of business, but I think that we need to think clearly what this means to the pocketbooks of consumers, especially consumers who in a state with an extremely high cost of living, are struggling to pay their rent, pay their mortgages, and whose wages are not going up.

We all do business with a huge variety of providers, or ISP, our wireless company, any number of online applications, and websites that we visit, and a significant amount of shopping. That's what people do. So potentially I am entering into transactions with hundreds of companies each year, many of which will be covered by CCPA. If each and every one of those companies is going to charge me an amount to opt out of the sale of my data, that's going to add up over the course of a year, and we get into a situation where we potentially run a risk of kind of two tier privacy law: One that works for the rich, who can kind absorb these fees on an ongoing basis and one that for poorer people, often frankly people who like me, I'm a non-profit worker, and I don't make big bucks, and my rent is a significant chunk of my salary and if you asked me to add a privacy budget each month or each year, it's going to be pretty limited, and the reality is I'm a privacy advocate, this is really important to me,
but the ability to be able to afford basically to act on your desires to prevent the sale of your data that in most cases people didn't even know about, but because of CCPA they will and they will have a choice, requires the ability to financially act on that choice.

We submitted to you some comments or some sort of regulatory protocols that you could consider in order to sort of balance these interests of people being able to afford to use the law and the legitimate concerns of businesses that are offering basically free services in exchange for data. I think we can meet that balance, but I want to be clear in what I wanted to sort of come here to say is it is a balance and the role of consumers that don't have unlimited resources for privacy, really needs to be front and center in your process. Thanks.

MR. MAUNEY: Any we are ready for comments in the 30s? If you have a comment card, 31 through 40, I suppose -- would you come on down to the front? As a reminder if you now decide you'd like to make comment, feel free to go and take a number and we can get you in later.

MS. SHELTON: Good morning. My name is (inaudible) Shelton and I'm a partner at Perkins Coie and first of all I want to echo comments that my partner, Jim Snell, just shared with you about the law.
In addition, one aspect I think that the AG's office regulations can help clarify is application or non-application of CCPA to purely employee related data and HR data. So there's confusion about the scope of the statute given that the definition of consumer's borrowed from the tax code and applies to the definition of residents into the tax code which is basically anybody in California for non temporary purpose, but when you look at the legislative history as well you know, talking to the components of statute and those are involved in the proposition pre-dated the statute, the focus was really on the consumer related issue and not management of personal data from an HR perspective. That's the area that I think regulation can be very helpful in clarifying and certainly a compliance standpoint for those companies who are not marketing their own employees. Some clarification on that issue would be very helpful.

In addition -- I know I won't take time here, we will be submitting comments on the specific items with respect to notices and a sort of making -- allowing for a safe harbor for businesses that are provided in the format that the AG's office might actually promote or set forth as to provide guidance so that companies are not subject to enforcement active or litigation activity, at least if they are not sort of a safe harbor with respect to the
notice of procedures and with that I will conclude my statement. Thank you so much.

MR. MAUNEY: Anybody else in the 30s? People are being surprisingly shy for a privacy forum here.

40s? Cards? Speakers? Go right ahead.

MR. OROZCO: Good morning. I'm Bernie Orozco on behalf the California Cable and Telecommunications Association, a trade association of members companies that provide video, voice and Internet service to millions of customers in California.

CCPA has been actively engaged in legislative activity related to the California Consumer Privacy Act and appreciates the opportunity to participate in these public hearings and the formal Attorney General rule-making that will follow.

At the outset I want to emphasize that CCTA and our member companies are committed to protecting customer privacy. Our goal has been and continues to be working with policy makers and learning from our customers to ensure CCPA is workable and will actually improve privacy protections.

We recognize that this AG rule-making and the 2019 legislative session will be underway simultaneously and that both offer opportunities for improved privacy protection under the CCPA.
Through additional legislative changes to the CCPA and through regulations we want to address significant operational issues that our member companies face to comply with the new law. We believe that a clear understanding of the operational and technical issues that result in regulations that are more feasible to implement and better protect consumers.

CCTA will be submitting written comments during this initial public participation phase and will participate when the Attorney General issues the formal notice of rule. Thank you.

MR. MAUNEY: Do we have anyone else who is prepared to make a comment?

MR. HOLMAN: Eric Holman from Santa Clara School of Law. I apologize, I'm not going to stick to the list that you have on the board but I don't think it makes (inaudible) among my peers here. I am a little surprised we don't have more comments because there is a lot of people who have plenty to say about this law. I've actually picked a topic that is not on this list, number one, target perspective for AG rule-making, clarify definition of business and when non California activity is counted towards the quantity threshold.

Right now, for example, the law applies to businesses that have 25 million dollars in revenue. It is
unclear if that means all 25 must be in California or if it means a single dollar comes from the California resident but all revenue is outside of the state. Similarly with the 50,000 consumers, it's unclear if that covers one consumer from California but 49,999 consumers from somewhere else.

So getting some clarity about when, in fact, you're counting activity outside of California toward this threshold would improve clarity about when non California businesses must comply.

A second tier issue I'm flagging for you, it is unclear if there is a ramp up time for compliance. Assume for a moment a business is at $24 million of revenue and then in a year it hits the $25 million threshold. Must they be in compliance on that day at which they hit 25 million dollars in revenue? And how would they do so? What if that revenue keeps fluctuating up and down? Must they always be prepared to be compliant when they're below the threshold? I would advocate for a period of time when someone hits the quantity threshold for the first time to phase in the requirements. That's not currently in the statute. I appreciate your time and attention and your hard work on this matter. Thank you.

MS. LANGSHEL: Good morning, Ellen Langshel, General Counsel for California Workers' Compensation
Institute. I shouldn't be here. This law should not apply to Workers' Compensation and yet it does. Workers' Compensation is already a heavily regulated industry and our members, which include both private insurers as well as self insured employers for Workers' Compensation are very concerned about the absence of a safe harbor and definition of sale, consumer and business. Thank you.

MR. MAUNEY: Anyone else like to come up?

MS. SCHESSER: We thought there would be more people who would be speaking but if nobody else would like to offer public comments I would like to reiterate again that you can always submit written comments to us at the privacy regulations at DOJ.CA.GOV mailbox as well as sending it to us via mail. Here's the address. And thank you all for coming and we look forward to continuing to hear from members of the public about our rule-making applications. Thank you.

(Public hearing ended at 11:08 a.m.)
REPORTER'S CERTIFICATION

I, Joan Theresa Cesano, Certified Shorthand Reporter, in and for the State of California, do hereby certify:

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

IN WITNESS WHEREON, I have subscribed my name, this 22nd day of January, 2019.

Joan Theresa Cesano, CSR No. 2590