CCPA PUBLIC HEARING

MODERATED BY NICKLAS AKERS

TUESDAY, DECEMBER 3, 2019

10:00 A.M.

RONALD REAGAN BUILDING

300 S. SPRING STREET

LOS ANGELES, CA 90013

(213) 830-7000

JOB NO.: 3609336

REPORTED BY: LUIS VAZQUEZ

PAGES 1 - 93

A P P E A R A N C E S

LIST OF ATTENDEES:

NICKLAS AKERS, SENIOR ASSISTANT ATTORNEY GENERAL

MIKE OSGOOD, DEPUTY ATTORNEY GENERAL

LISA KIM, DEPUTY ATTORNEY GENERAL

ELEANOR BLUME, SPECIAL ASSISTANT TO THE ATTORNEY GENERAL

SPEAKERS:

MARSHA MATHIAS, DIRECT GOVERNMENT RELATIONS, KINECTA CREDIT UNION

CRYSTAL HAASE, USE CREDIT UNION

NARA HARTMANN, USE CREDIT UNION

STAN STAHL, PHD, SECURETHEVILLAGE

SARAH THOMPSON, SIEMLY GLOBAL

JESSICA GROSS, ATTORNEY

JUSTINE M. PHILLIPS, ATTORNEY, SHEPPARD MULIN

DAVID GREELEY, ATTORNEY, GREELEY THOMPSON LLP

JOSEPH GARIBYAN, ATTORNEY, STYSKAL WIESE & MELCHIONE LLP

MARY-LOU HEIGHES, PRESIDENT, COMPLIANCE PLUS INC.

PETER WATSON, GENERAL COUNSEL, US STORAGE CENTER & CSSA

TANYA FORSHEIT, CHAIR OF PRIVACY GROUP, FRANKFURT KURNIT KLEIN & SELZ

A P P E A R A N C E S (CONT.)

JEFFREY M. DENNIS, PRIVACY ATTORNEY, NEWMEYER DILLION

LEIGH MCMILLAN, CEO, WHITEPAGES

SCOTT MCELROY, PAYLIDIFY

ROMAN HOSSAIN, REVIEW SQUASH

DAVID GRIMALDI, EXECUTIVE VICE PRESIDENT, THE INTERACTIVE ADVERTISING BUREAU

BO W. KIM, ATTORNEY, PERKINS COIE

PHILIP RECHT, MAYER BROWN LAW FIRM

ROSS COHEN, CO-FOUNDER, BEENVERIFIED

JASON MATTHES, GENERAL COUNSEL, SPOKEO

DAVID LEVINE, PRINCIPAL, GROOM LAW GROUP

KEVIN WALSH, PRINCIPAL, GROOM LAW GROUP

FIELD GARTHWAITE, CO-FOUNDER AND CEO, IRIS.TV

DR. MAXINE HENRY, PRESIDENT, CYVIENT

P R O C E E D I N G S

MR. AKERS: My name is Nick Akers. I'm the Senior Assistant Attorney General in charge of Consumer Protection in the California Attorney General's Office, and I'll be the hearing officer for today's proceedings. Also present with me here today are Deputy Attorney General, Mike Osgood, Deputy AG Lisa Kim, and Special Assistant to the AG, Eleanor Blume.

For the record, today is the 3rd of December and the time is 10:00 a.m. We are at the Ronald Reagan State Building in the auditorium at 300 South Spring Street, Los Angeles, California.

Before we begin, there are a few points that I'd like to make.

The notice of proposed rule-making for the CCPA regulations was published in the California Regulatory Notice Register on October 11, 2019 in Register No. 41-Z, starting at Page 1341. The notice and relative rule-making documents were posted on the Attorney General's website on October 10, 2019 and were mailed to all interested parties who'd requested rule-making notices. Today is the second of four public hearings that were announced in the notice.

The deadline for submitting written

comments is this Friday, December 6, 2019 at 5:00 p.m. Pacific Time. We recently posted additional resources on or website about the DOJ's CCPA rule-making process including two documents in PDF format titled, Tips on Submitting Effective Comments and Information About the Rule-making Process. And if you visit oag.ca.gov/ccpa, they're posted there, and there is further information.

Today's public hearing is quasi-legislative in nature, and it's being held pursuant to the California Administrative procedures Act. The Administrative Procedures Act specifies that the purpose of this hearing is to receive public comments pertaining to the proposed regulations.

If you're speaking today, we ask that you limit your comments to the proposed regulation or the rule-making procedures that we're following. We do not intend to answer questions or otherwise engage in dialog in response to any oral or written comment, however, we may ask that you speak slower or louder or ask limited follow-up questions just to clarify a point.

Today's hearing is being audio recorded, and it's being transcribed by a court reporter. The transcript of hearing and any written

comments presented during the hearing will be may part of rule-making record.

If you are speaking, please try your best to speak slowly and clearly to help the court reporter to create the best possible record. If you brought written comments that you'd like to submit during the hearing today, please give them to a staff member at the sign-in table.

After the public comment period ends, the Department will review and consider all relevant comments and recommendations provided at the public hearings and in writing. The Department will then compile a summary of each relevant comment or recommendation and prepare a response to it, which will be included in the Final Statement of Reasons. Once the Final Statement of Reasons is complete, the entire rule-making record will be submitted to the Office of Administrative Law, and a copy of the Final Statement of Reasons, along with the notification of any changes made to the proposed regulations, will be posted on the Attorney General's website, again, at oag.ca.gov/ccpa.

We're required to notify all persons who provided a comment, and all those otherwise interested of any revisions to the proposed

regulations, as well as any new material relied upon in proposing these rules. Accordingly, there's a check-in table located outside of this room, just off to the left, where speakers and attendees can sign in and provide their contact information. You may sign in to speak without providing your name or contact information, however, please know that we then will not be able to provide you with notice of revisions to the rules or other rule-making activities.

If you intend to speak at today's hearing, you should have received a number when you signed in. When we call your number, please come up to the microphone, and if you'd like to be identified, state and spell your full name and identify any organization you represent. If you have a business card and you could provide a copy of it to the court reporter before approaching the microphone, that would be appreciated.

Each speaker will have five minutes to speak. To assist the speakers, Deputy AG Osgood will hold up a card to alert the speaker when they have one minute remaining. In the interest of time, if you agree with comments made via prior speaker, we'd encourage you to just state that fact, and then add any new information you believe is pertinent to the

issue.

Also, there is no need to read aloud written comments that you're submitting. All comments, whether written or oral, will be reviewed and responded to by our office in the course of the rule-making process.

If we have remaining time after all the speakers have had a turn, we'll give speakers an opportunity to take a second turn and add to their remarks.

If you'd like to make an oral comment today and have not yet received a number, please go ahead back out to the check-in desk and get a number, and that'll help us keep this organized.

Lastly, we'll need to take breaks during the proceeding including at least a 30 minute lunch break for our court reporter. If it appears that we have no speakers waiting for their turn, we also may end the hearing before the lunch break or at some point before the end of day.

At this time, if I could have the first speaker come to the microphone.

Good morning.

MS. MATHIAS: Morning.

MR. AKERS: Yes.

MS. MATHIAS: Good morning. My name is Marsha Mathias. The spelling is M-A-R-S-H-A, and the last name is, M-A-T-H-I-A-S, and I represent Kinecta Federal Credit Union in Manhattan Beach. And I thank you for hearing our concerns today about the CCPA.

Kinecta is a non-profit financial cooperative that serves the financial needs of our 247,000 members throughout California and protecting their non-public, private information is very important to us.

Our two concerns that I'd like to share -- the first is with the exception of the consumer liability provisions for a data breach of any non-encrypted or non-redacted personal information, the entire CCPA does not apply to personal information collected, processed, sold, or disclosed pursuant to the Federal Gramm Leach Bliley Act or the California Financial Information Privacy Act. The proposed regulations do not incorporate references to this exemption. It's imperative that the final regulations incorporate references to the GLBA and CFIPA exemptions specifically identifying the categories of information not covered under those two -- the GLBA and the CFIPA. Many businesses such as Kinecta have built strong consumer friendly privacy programs based

OLA 1-1

on the requirements set up under the GLBA and the CFIPA, and those companies should be allowed to leverage our existing compliance activities to benefit our members.

OLA 1-1 cont

The second concern regards the four notices that are required under the proposed regulations. For all the required notices, the proposed regulations require that the notices be easy to read and understandable by the average consumer and provide some standards to achieve that. This direction is subjective and does not contemplate a method or metric to assess the readability.

OLA 1-2

Since all businesses need to provide the required notices, the creation of uniform model notices would help to ensure consumers' understanding of the notices. It would simplify the requirements for businesses and create an objective review on whether the businesses' notices meet the required standards.

Thank you that's all of my concerns. We'll be submitting written ones as well.

MR. AKERS: Thanks very much.

MS. MATHIAS: Thank you.

MR. AKERS: Speaker No. 2?

MS. HAASE: Good morning. My name is

Crystal Haase, that's H-A-A-S-E, and I'm here from USE Credit Union, another financial institution similar to Kinecta. We appreciate the opportunity to speak today. I have a couple of comments on the proposed regulations.

First, while we fully agree with the concept of consumer rights to request information, operationally, we are concerned with how we will satisfactorily comply with those requests, particularly as it pertains to our non-members -- or, I guess, this would be non-customers for the regular industry. For example, when a non-member uses one of our ATMs, while we gather the necessary data from the individual to process that specific transaction, that data is very limited, and therefore, provides challenges to adequately verify the identity of a requestor of information.

OLA 2-1

And secondly, as far as the notices similarly to Kinecta's comments, with the notices and disclosures required under the CCPA, there is no model language or form notices for those disclosures. It would be helpful for us, not only for businesses to utilize model language, but also to standardize those communications for consumers to more readily understand what is being shared with them. And like

OLA 2-2

with many model notices and sample language, we would like to request some sort of safe harbor if those models are used.

OLA 2-2 cont

Thank you

MR. AKERS: Thanks very much. Speaker No. 3, please.

Good morning.

MS. HARTMAN: Good morning. My name is Nara Hartmann. It's N-A-R-A, Hartmann, H-A-R-T-M-A-N-N. I'm also here from USE Credit Union in San Diego.

First, I'd like to say that USE Credit Union is a champion of consumer privacy rights, and we certainly support the enhancement of those rights through bills like the CCPA. The financial industry, of course, has several privacy protection laws in place, and we have for several years. We appreciate that exceptions were built into the proposed rules for CCPA regarding information already covered by GLBA and the CF- -- I'm going to get lost in that -- CFIPA. I think I got it. I like the idea that it's intended to carve out what's already covered and enhance those rules already in place.

OLA 3-1

My concern is that by creating another privacy law, this is going to be another communication

that goes out to members. So they already receive a policy and notice under federal law. This -- they already receive one for state law, and this will be a second state communication. So there is already a lot of confusion and questions that come in from members about that. So it's going to be, I think, even harder for them to understand what the rules are and how to really take advantage of their rights under those rules.

OLA 3-1 cont

Under the proposed rule, verifying the identity of individuals for whom we hold limited information will be a significant challenge. For example, when a beneficiary is listed on an account, we may only have their name. So if we receive a request for information from someone with that same name, we really would have no way to connect that those people are the same person. If the data is being protected in the same manner that we would treat our members data under California privacy laws already in place, the FIPA, will not be sold and cannot be deleted due to retention requirements, then perhaps the confirming for consumer that the information exists is a pretty difficult effort assuming that verification is even possible.

OLA 3-2

Although some exceptions are included,

again, for information covered under federal and state laws, there are unique situations that will be very burdensome for us. For example, non-member information collected while processing transactions. Let's talk about, like, the maker of a check. So we receive thousands of checks each day deposited to our members' accounts. The maker information on each of those checks is certainly somebody's private information under the rules. However, we don't have any way to search that information. It information is stored by image only. So if we received a request for information for a 12-month look back period, we would be searching images of every single item for every single day that checks were deposited. That would be pretty -- very, very burdensome.

OLA 3-2 cont

So again, we would just ask that some consideration be made for information that might be on file if it's already protected in the same manner as our members' information that's not able to be deleted or destroyed due to retention requirements and will never be sold.

Thank you.

MR. AKERS: Thank you. Speaker No. 4, please. Speaker No. 4?

Good morning.

MR. STAHL: Good morning. My name is Stan Stahl, S-T-A-N, S-T-A-H-L. And I'm -- want to speak about the CCPA, and what one would call minimum reasonable security practices. I speak as the founder and president of a California non-profit, Secure the Village. We're a community of information security practitioners, IT vendors, and MSPs, attorneys with practice in cyber, cyber investigators, insurance and risk management people, law enforcement including the FBI, secret service, both the LA County and Orange County District Attorney's Office are part of our organization and others. In addition to our base here in Los Angeles, our community expends to Orange County and Sacramento. OLA 4-1

The experience and expertise of our organization's members runs very deep. Speaking personally, I entered the field of computer security in 1980 as a young PhD in mathematical logic from the University of Michigan. In those early years, I was privileged to work securing advanced technology systems for the White House, Strategic Air Command, NASA, and other national assets.

Seven teen years ago, I co-founded an information security management firm, Citadel Information Group, to assist mid-market and smaller

organizations manage their information security needs.

In the nine years prior to founding Secure the Village in 2015, I served as president of the Los Angeles Chapter of the Information Systems Security Association.

I speak to you today regarding the CCPA's right of compensation to consumers in the event of a data breach, except when the breached business maintains "reasonable security procedures and practices appropriate to the nature of information being protected." As has been widely discussed, there's a great deal of uncertainty as to exactly what reasonable security procedures and practices is to mean. In response to this uncertainty, Secure the Village has developed and published, as a free public service, a set of, what we consider to be minimum reasonable information security management practices. And these are available on the Secure the Village website, securethevillage.org.

For the reasons we describe below, we invite you to use our minimum reasonable information security management practices in assisting California establish appropriate reasonability requirements for organizations to follow in complying with CCPA and other information security management obligations as

OLA 4-1 cont

well. As you know, they exist in other places in the law.

We view these minimum reasonable practices as so basic to the responsibility of securing private consumer information that a failure to implement them should be considered prima facie evidence that an organizations information security procedures and practices are not reasonable. We developed them to be commercially reasonable and reasonably achievable for any company subject to CCPA.

It's important to note that we're not saying that an organization meeting these minimum practices has reasonable practices. To cite one example, the reasonability requirement for a large telecommunications company or internet service provider is considerably more than our suggested minimum. And even a company that meets our minimum standards might still not have reasonable standards of "appropriate to the nature of the information being protected." Our suggested minimum is designed to establish the floor, not set the bar. That's an important point with what we've done.

Our minimum reasonable information security management practices are based upon other existing information security standards. These

include the NIST Cyber Security Framework; the International Standards ISO 27001, that whole family; the Center for Internet Security's Critical Controls; the New York State Department of Financial Services cyber security requirements for financial services firms. Does that mean I have a minute?

MR. OSGOOD: You have less than a minute.

MR. STAHL: Less than a minute, let me go -- okay. So our practices are based or nine elements. I'm not going to go into them. You'll get this later. I just do want to point out that in 2016, as you know, then Attorney General, Kamala Harris, in the California 2016 Breach Report looked at the CIS 20 as a minimum. We feel those are both too weak in some cases, and too strong in others. And that's why we much prefer that you use ours -- you know, our standards.

And so, just to go on -- I mean, I saw Mike -- your thing -- let me finish then. And just say, please take a look at these. We invite you to look at them, consider them, and include them as you're making decisions as to what is to count as reasonable security practices and procedures.

Thank you very much.

MR. AKERS: Thank you, sir. Speaker No. 5.

MS. THOMPSON: High there. My name is Sarah Thompson. I'm representing Siemly Global, and we are the creators of a platform that helps companies handle consumer privacy requests, so data subject access requests for GDPR and the like. And so we are speaking to a lot of customers and potential customers, a lot of financial institutions regarding this regulation, and there's a few things I want to talk about today.

One is about, you know, who should be a covered entity. Identity verification and the execution of Right to Know and deletion requests.

So first of all, I'd like to start off with just some, you know -- we're getting some -- there is some obvious people there are -- or companies that are covered by CCPA, but there is also some not so obvious. And some of the questions that have come up are businesses that have over 50,000 -- collect over 50,000 consumers' data that do get their profits from things like Google ads. So they could sometimes get 100 percent of their profits from Google ads. In effect, if they are -- their question is are they, in effect, selling that data, and are then they supposed

OLA 5-1

to be covered by CCPA? So that's a big question that's come up.

Another question has come up actually from non-profits which is, you know, we know that it states it is a -- you need to be a for-profit business to be covered by CCPA. But non-profits do collect a large amount of information from a large amount of Californians, so there are question about, you know, what, if any, practices or if they have to comply with this in any way. So that's kind of about -- those are my questions regarding who should comply.

Now regarding the executions of the Right to Know and deletion requests, there's a few questions that have come up. The ambiguity of some of the language. You know, we have some language that states that, you know, we have to make sure that we transmit our Right to Know, and deletion, and any type of information with the consumer in a secure manner, but that's not really identified, like, what that is. And so, you know, there's questions like is that an email? Is email okay? Or are we -- or businesses, will they need to create a secure login to a third-party platform for them to be able to access information?

So what we don't want to do is

OLA 5-1 cont

OLA 5-2

OLA 5-3

basically cause a breach by sending emails to consumers which can definitely happen when we're talking about non-customer data. So -- which is something a lot of companies are concerned about. So you just have an email address. You don't have any other secure portal to communicate. How are you supposed to communicate securely? So we'd like some clarity on that.

OLA 5-3 cont

We also have some questions regarding, like, what is the requirements from an organization to remind our -- the consumer to confirm their request? So if a consumer submits a request, there is language that states that they -- if it's a request for deletion, that they have to actually confirm it a second time. If they do not confirm it, does the -- does the organization have to remind them? Do they -- how many reminders can they send? Can they close the request after a certain period of time? What is their obligation there?

OLA 5-4

Other questions that are coming from execution in regard to deletion of data. It is specified that in reference to archived or backup system, you mentioned that it doesn't need to be deleted until it's next accessed or used, which is an ambiguous term in IT. So that would -- we'd

OLA 5-5

definitely like to have that clarified. We have a lot of customers that are worried about that. As well as, you know, what does it mean to specify the manner in which data is deleted? So what does that mean?

OLA 5-6

Finally, in regards to request for deletion, we have a lot of customers that are third-parties, and they want to know, like, what they can expect when a company receives a right to deletion. Do they need to convey that to the third-party at all? Does the third-party -- are they required to, you know, let the company know that they've complied at all for the deletion request? Or is it -- does the consumer have to make a request to each individual third-party?

OLA 5-7

And finally, what is a reasonable degree of certainty when you're looking at age -- identity verification? And I just want to sneak this one in here. Proof of age verification for opt-ins, does that not mean that everyone will have to have a proof of age verification to say that they are indeed a -- they are an age of majority and not a minor? And if so, does that require an actual identity verification tool in order to do so? So how do you actually verify age, or is this simply a check box that they can check? So these are questions that

OLA 5-8

are -- that we'd love to have some clarification on.

Thanks very much.

MR. AKERS: Thank you. Speaker No. 6, please.

Good morning

MS. GROSS: Hello, my name is Jessica Gross. I am an attorney helping many, many, many companies try and deal with this law. Thank you very much for the regulations. They add a lot of clarity to what was already tons of inconsistencies and subdivisions to nowhere if anyone's dealing with this.

So I'm here to plead and beg for some kind of clarity on what the term "valuable consideration" means. Under 1798191 Subdivision B2 in the CCPA, the Attorney General has the power to adopt regulations that are necessary the further the purpose of the title. In the proposed regulations, we do have some definitions, and the initial statements of reasoning say these definitions were provided to add clarity to ambiguous terms like categories of third-parties, for example.

"What is a sale?" is an ambiguous term that I'm sure you've heard. This is argument before -- there's articles all over the place on what kind of a data exchange is going to qualify. It's

OLA 5-8 cont

OLA 6-1

important because a covered business is going to have to be able to understand how to classify what these third-parties are, what their service providers are -- two terms that are also fraught with some inconsistencies. And when are they going to classify those disclosures as something that's a "sale" when they're selling, renting, releasing, disclosing, disseminating, making available, transferring in any way for monetary or other valuable consideration?

OLA 6-1 cont

California Civil Code 1605 defines consideration as, "Any benefit conferred or agreed to by -- conferred to by the promisor or by the promisee." So what separates "valuable consideration" from just consideration? And how are we to deal with situations where the company is paying another company for what appears to be a service, and what is actually listed as a business purpose in 1798.140 Subdivision D, which would be something like verifying the quality of ad impressions and auditing compliance with specifications? Or performing services like providing advertisements, marketing serves, and analytic services. But we've all heard the debate with things like Google analytics, for example, is selling information.

OLA 6-2

We, please, ask and request that there

is some kind of factor test -- any kind of clarity whatsoever, that describes kind of where that line is between a disclosure for that business purpose. And hopefully, yes, if the company does not further use the information in some way, you could argue perhaps they're a service provider. But if the contract doesn't meet the right specifications, which many service providers do not want to sign, then you don't get to really ride that exception.

OLA 6-3

This creates a really big problem for businesses who now have to put a button on their webpage, or explicitly list in in their privacy policy that they do not sell. That's going to open them up to violations that in the CCPA, if they fail to interpret that correctly, and it could also stand for UCL violations, FTC violations, or other issues of misrepresentations made in a privacy policy.

But how are we to make sense of what a "consideration," or "valuable consideration" is when the California Court of Appeal in, In Re Fremont Estate said that, "Value can mean whatever. A peppercorn, a tomtit, or even at a dollar in a hand."

Thank you.

MR. AKERS: Thank you. Speaker No. 7, please.

Good morning

MS. PHILLIPS: Good morning. Justine Phillips here, attorney in cyber and employment at the Law Firm of Sheppard Mulin. I want to echo Speaker No. 4 and No. 6's concerns with respect to the need for reasonable security definition and framework. Obviously, New York has selected a regulatory framework and perhaps guidance can be gleaned from that. Also, on the valuable consideration, huge issue that we're also dealing with.

The issues with respect to AB25, we understand that the regulations were drafted before AB25 was passed. And, in fact, the day after the regulations were released, AB25 went into effect. AB25 requires that employers give some disclosures on January 1, 2020. This has left certain disclosures and the notice provisions in the current regulations insufficient for guidance for employers to the extent that additional guidance can be given with respect to AB25 and what should be disclosed to employees in the minimal initial at collection can be confusing. The applicants obviously are going to be a separate stand-alone disclosure, likely something to happen during on-boarding or in the application process. With respect to employees, perhaps an employee

OLA 7-1

OLA 7-2

OLA 7-3

handbook or policy provision would be sufficient, or perhaps an independent online notice for employees to visit, so they can also provide some notice and disclosure to those third-parties and emergency contacts that are identified by employees. These are two groups of people that are quite difficult to impart a notice to even though they are afforded some protections under CCPA.

OLA 7-3 cont

Thank you.

MR. AKERS: Thank you. Speaker No. 8, please.

Good morning

MR. GREELEY: Good morning. David Greeley. I'm an attorney with Greeley Thompson LLP in San Diego. Just two quick comments.

Under the Regulations 999.305D, it provides that a business that does not collect information directly from consumers does not need to provide a notice at collection to the consumer. That regulations makes a lot of sense, and I'd ask that you consider having that same caveat in Regulation 999.308, entitled "Privacy Policy." It seems like it's a similar situation. I'd ask you to consider that.

OLA 8-1

Secondly, I just have a comment about

service providers. There is a section in 999.314C, it states, "A service provider shall not use personal information received from a person or entity it services, or from a consumer's direct interaction with the service provider, for the purpose of providing services to another person or entity." And I'd ask for clarification that if the service provider also meets the definition of a "business" and such business/service provider otherwise complies with the CCPA, that that limitation would not apply. That that's meant to apply to a service provider that is not a business.

OLA 8-2

Thank you.

MR. AKERS: Thank you. Speaker No. 9, please.

Good morning.

MR. GARIBYAN: Joseph Garibyan. I'm a -- I'm an attorney with the law firm of Styskal Wiese & Melchione. We represent financial institutions primarily credit unions, and I know the first several speakers represented credit unions. And we're -- we would like some -- really clarity on the CCPA's application specifically on credit unions for primarily two reasons.

The first one, you know, which was --

which struck out to me was from the Attorney General's initial statement of reasons I saw on Page 21. The Attorney General took the position that non-profits are clearly not subject to the CCPA. But the definition of business in the statute defines -- includes, "any legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners."

Now credit unions specifically California state Charter Credit Unions are actually formed under the corporation code as non-profit mutual benefit corporations. So you can have non-profits that function and operate for the financial benefit of their owners, which in the credit union space, they're referred to as their members which in banking they would be their depositors. So that has, you know, inserted some confusion about whether or not this particular industry is subject to the CCPA.

OLA 9-1

The second thing is -- which I believe during our last meeting I previously commented on and asked for some clarification, was that the GLBA and the SB-1 exemption -- because the statute currently reads that, "data that is collected pursuant to GLBA and SB-1," which comprises of probably most of the data that financial institutions collect from their

OLA 9-2

depositors. It's a fairly broad statute -- is exempt, but the way it's written is it leaves open the possibility of data that is not collected pursuant to those statutes to be subject to the CCPA.

So my question is if we can get some clarification as to whether or not that particular provision was intended to be a financial industry exemption, or are we just talking about data? And in reviewing AB -- I think, 1202, which is, I think, for data sellers, the exemption was much more clear that it applies to financial -- the financial services industry as opposed to the data that they collect specifically. As well as if you can draw from an example from Nevada, they specifically carved out in their privacy regulations financial institutions as a whole.

OLA 9-2 cont

So for this particular industry, particularly credit unions, there are two elements that are adding confusion, and it's very difficult to establish a compliance program where you're dealing with, you know, disclosures under the GLBA, SB-1, CAL OBA, and you have to harmonize all those statutes, and they all to different things with data, and actually disclose to your membership, customers, depositors, the public at larger, what in fact you're doing with

your data. Because you're redirecting them to different statutes and policies. So if we can get some classic clarification as to that, it'll, you know, make, you know, the compliance people at these institutions very happy.

Thank you.

MR. AKERS: Thank you. Speaker No. 10, please.

Good morning.

MS. HEIGHES: Good morning. My name is Mary-Lou Heighes, and I am the president of Compliance Plus Incorporated, which, as the name implies, I am in charge of compliance training and consulting for credit unions and small community banks.

A couple of things that my clients in particular are finding very difficult to deal with in putting these regulations and this law into practice. We already have Gramm Leach Bliley as you know. We already have SB-1 as you know. When we are trying to actually implement -- so it's very different as a speaker when I get up in front of people, and I say you need to do this, and you need to do that, and it's going to be a spreadsheet, and it's going to be a big spreadsheet to having a client walk up it to me and says, "Mary-Lou, you need to come in my office, and

OLA 9-2 cont

you need to do this for me." So I have first-hand experience at trying to get all of these moving parts, and there's a lot of moving parts, together.

So a couple of issues that are of particular concern. In your regulations, specifically, 305(e), it talks about offline collection, which I understood from the regulation -- I mean from the law immediately, that this law would apply in an online and an offline environment. Then going into an institution and actually finding out all of the different ways that people are collecting information, anything from a raffle ticket or trying to get new account holders by having a referral program, for example. There would be no way to catalog -- we are not keeping this information in an electronic environment -- there would be no way to catalog or even be able to recover that information.

OLA 10-1

Essentially, in these referral programs, for example, we'll have a branch conducting a specific promotion where they will pay an account holder $10 to refer a family member or friend. If that family member or friend obtains an account, they too get $10. That goes into, essentially, a box that sits in the branch manager's office. And maybe they'll send out a letter to that person saying, hey

you know, you've been referred to the credit union, you've been referred to the community bank. You know, would you like to, you know, come in and open an account, or you can send back this application. And they might hold on to it for three or six months. And then we reach out to them or use it to verify who was the referring party. That information -- there is no way for us to go and get that information later on when we get a request from a consumer. That's going to be very difficult. And there's a number of other examples. I'll be submitting written comments to that effect.

OLA 10-1 cont

The second part of that is, again, the GLBA exception, the SB-1 exemption, that is very important from a financial institution aspect is to -- I'm trying to differentiate for my clients what is information that is covered by those exemptions, and what information is covered by CCPA.

So to the extent that we are looking at that, I'm going to reiterate the comments by USE and a couple of other comments that were made, is when we need to process the transaction -- the ATM example is the perfect example, or I'm going to write Mr. Akers a check, and he's going to deposit it at his institution. Now his institution has my personal

OLA 10-2

information on it including my account number. And then when that check gets processed back to my institution, I can see that he cashed that check. And if he wrote his account number on the back of that check, I would then have his name and account number as well as the financial institution where he has an account.

So all I'm asking is to reiterate what the previous speaker said and what USE said as far as the GLBA exemption, that it applies to all consumer information that is necessary to process, effect, enforce, or administer a transaction.

We also have issues when it comes to collections, for example. When a collector is gathering information much like an investigation or a law enforcement investigation, you have your subject. In our case it would be our borrower. They're a skip. They're not paying. They have a vehicle that we need to repossess, for example. We're getting information from other consumers -- their phone number, their address, or whatever -- in an effort to locate our skip and to locate our vehicle. We get an address for the girlfriend. Well, maybe the car is over there. So now we have information about a consumer, but the only reason why we have the information is to

OLA 10-2 cont

OLA 10-3

basically effectuate this contract that we have with our consumer who received the GLBA notice, but this other person did not.

And so, we want to look for an expansion or a definition, that we were hoping for originally, that would mean that anything that we obtain that is necessary to process or facilitate a transaction is, in fact, covered that transaction when it's not, in fact, shared for any other -- or utilized for any other purpose.

OLA 10-3 cont

So those were the main things. We have things like requirements for a currency transaction report. We have a non-member that walks in, deposits $11,000 in cash to an account holder's account. We need to collect information, by law, about their driver's license, their name, their address, their taxpayer identification number, but they're not our account holder, and there is no specific exemption for information required by law.

OLA 10-4

My final comment in the last minute, would be that that 45-day and 90-day period for responding to consumer complaint -- or consumers is very important because we do not house -- and I say -- we is my clients -- do not house everything in a nice little neat database that we can just go in -- do we

OLA 10-5

have Mary-Lou Heighes on file anywhere? Information is stored in a lot of different places, and it's very difficult to, you know, comply in a shorter timeframe.

Thank you very much.

MR. AKERS: Thank you. Speaker No. 11, please.

Good morning

MR. WATSON: Good morning. My name is Peter Watson, P-E-T-E-R, W-A-T-S-O-N. I'm the General Counsel for US Storage Centers, a privately owned self-storage management company, as well as a member of Board of Directors of the California Self Storage Association, CSSA, which is a non-profit association predominantly comprised of self-storage owners, operators, and vendors. I'm presenting my comments today as a representative of both entities. I want to focus my limited time on really one threshold issue, and if there is more time to touch on a couple of regulations, I'll try and do so.

Specifically, I'd like the Attorney General to consider limiting the scope of the defined term, quote/on quote "personal information," solely as that term applies to the 50,000 consumer threshold set forth in Civil Code Section 1798.140 Subdivision CB. As currently drafted, the general consensus is that

OLA 10-5 cont

OLA 11-1

any California resident that accesses a business' website will automatically be considered a consumer providing personal information under the Act simply because the IP address utilized to access such website will be cached by the business. To use a basic hypothetical specific to the self-storage industry, imagine the self-storage property management company that receives annual website traffic from 50,000 IP addresses but only services and collects non-IP address personal information from, say, 10,000 consumers. Those would be their tenants, prospective tenants, folks that go online and provide their email address or contact information to be contacted for any reason. Those are the 10,000. Should this smaller size operator with 10,000 customers be subject to the CCPA? More importantly, how does this company know whether they're subject to the CCPA? Do they have the ability to find out how many IP addresses their website has received in any given year? And if so, than can they take that list of IP addresses and determine which of those IP addresses are California IP addresses? Assuming yes, can they then determine which of those California IP addresses are not also their existing tenant base? Most folks that are accessing the website could very well be the tenants,

OLA 11-1 cont

and you don't want to have a double counting situation to determine whether or not you're subject to the law.

It seems to me that this hypothetical company is not the intended target of the CCPA. It's far removed from the larger businesses and types of businesses that, I believe, the CCPA was enacted to govern. Nevertheless, the mere receipt of IP addresses arguably brings this company under the CCPA purview. I refer to this situation as the quote/unquote "IP address-only consumer scenario," and imagine that this issue and concern is at the forefront of a vast number of many smaller to medium sized businesses that are scrambling to determine whether they need to comply with the CCPA as a result of the quote/unquote "IP address-only consumer scenario," and, of course, determining the best way to comply in a timely fashion.

OLA 11-1 cont

Under this context, I urge the Attorney General to consider and hopefully implement one of the following proposed regulations:

The first proposal, and the preferred approach, would be to specifically exclude IP addresses from the definition of personal information solely as it pertains to calculating the 50,000 consumer threshold. This would not remove IP

addresses from the definition generally, again, only from the 50,000 threshold calculation. This proposal, if implemented, would eliminate the IP address with respect to the "IP address-only consumer scenario" and provide clarity for businesses that are unable to determine if they are subject to the CCPA.

OLA 11-1 cont

As an alternative to the first proposal, I would ask that the AG consider removing the consumer's right to request deletion of personal information for businesses that would not qualify under the 50,000 consumer threshold, but for the mere collection of IP address-only consumers. Under the second alternative, the consumer will still have the Right to Know via the business' privacy policy. However, the consumer will no longer have the right to request deletion. Okay. Thank you.

OLA 11-2

Now as for a couple of other regulations. The definition of household, the one comment here would be to perhaps clarify the situation where you have a mixed use -- or not mixed use, but mixed residency house who have people from California, people from other states, and how to treat those folks from other states that are within that particular household.

OLA 11-3

Section 999.312C, I ask that the CCPA

OLA 11-4

should not treat businesses differently. Businesses that have an online presence and a brick and mortar presence versus those that have just one or the other, it seems that under that particular section, there is two different standards.

Thank you for your time.

MR. AKERS: Thanks very much. Speaker No. 12, please.

Good morning.

MS. FORSHEIT: Good morning. Tanya Forsheit, Frankfurt Kurnit Klein & Selz. I'm the chair of the privacy group. I'm here actually today testifying on behalf of my client, The News Media Alliance. The News Media Alliance represents nearly 2,000 diverse news organizations in the United States from the largest and international outlets to hyperlocal news sources both digital and print.

When businesses succeed at CCPA compliance, consumers will win. As such, the Attorney General should approach the regulations in a manner that is designed to help businesses succeed. The alliance's comments today are focused on those areas where the regulations make compliance much more difficult than what is anticipated in the statute, if not impossible in some cases. Most of these issues

OLA 11-4 cont

arise in situations where the draft regulations impose new obligations that were not set forth in the statute itself. I'm going to provide just a few examples that are of particular interest to The alliance.

First is the notice at collection requirement, which is set forth in the regulations. This is new. It's not in the statute, and it is unclear, particularly for publishers, will make things even more complicated for consumers who already have to navigate a number of links and notices on websites. The language would require a new link. This would be in addition to the privacy policy, as we understand it as set forth in the draft regulations. So consumers will not understand the difference between the two, privacy policy, notice at collection. I mean, the privacy policy does, of course, include information about how information is collected. It's required to do so. It will normally have a subheading to that effect. This would also be in addition to the "do not sell my personal information" link. So what we're already imaging is privacy policy, notice at collection, "do not sell my personal information," never mind all the stuff that's already out there about ad choices etc. It's not clear where this link should be placed, the notice at collection link, if

OLA 12-1

that's what's required. And whether it should appear at or before the time of collection. And there's some inconsistent language in the regs as to whether it's at or before.

So respectfully, The alliance submits that there's no need for an additional link. If it is required, it should be at and not before the time of collection. Before would essentially create and opt-in obligation, which is inconsistent with the statute. And if it is required, the obligation to post should be delayed -- in other words, if there is a link requirement -- a separate link, that should be delayed until January 1st, 2021, given that the regs won't be finalized until the summer.

OLA 12-1 cont

If a business -- so that's the point about the notice at collection. Second point, if a business is not selling information, and I'm not going to get into what's a sale, but if it's not selling, it should not be required to post a "do not sell my personal information" link. There is some language in the regulation suggesting that if you might, in the future, sell information, you need to have that link. That, of course, would be extremely confusing to consumers and also not provide transparency. Any business might theoretically start selling information

OLA 12-2

in the future. They shouldn't have to have a link if they don't do it. Of course, if they change their practices, they should put one in place before they start doing it.

OLA 12-2 cont

Number three, the regulations should not require that an unverified deletion request be treated as an opt-out of sale. That is not in the law. It's also fraught with potential for abuse from automated bot attacks to submit thousands of unverified deletion requests that would theoretically have to be treated as opt-outs. What if the business doesn't sell information? And how are they supposed to effectuate the opt-out if they can't verify where these are coming from if they're automated bot attacks. There shouldn't be a separate requirement to treat those as opt-outs. If you can't verify a deletion request, you shouldn't be required to honor it.

OLA 12-3

Next, the do not sell request should be honored when a consumer clicks on do not sell. There is language, of course, in the regulations about having to treat things like user privacy controls or browser controls as a do not sell request. This is not in the statute. Also, it would be extremely confusing because businesses can't possibly

OLA 12-4

operationalize it. It should be simple. A consumer clicks on do not sell, that means do not sell. There's an opt-out. That would conflict. What if they later click on the other browser control, or they're using a do not track, or whatever it is, impossible to operationalize if both are required and confusing for consumers.

OLA 12-4 cont

Service providers, that was mentioned by some others, but as long as the service provider is only using information to provide service for businesses purpose -- my time is up -- it shouldn't matter if they're using the same information from two different businesses. That's not in the statute. IP addresses are frequently used from two different businesses. For example, for frequency capping and advertising. That's a consumer protective service. If you can't be a service provider for that purpose, and you require that to be an opt-out, that creates complete chaos.

OLA 12-5

I'm out of time. Thank you very much. I appreciate it.

MR. AKERS: Thank you. Speaker No. 13, please.

MR. DENNIS: Good morning.

MR. AKERS: Good morning.

MR. DENNIS: My name is Jeff Dennis, D-E-N-N-I-S. I'm a privacy attorney with the law firm Newmeyer Dillion in Orange County representing a number of companies who seek to comply with the CCPA. I have a few just brief comments and thoughts. I appreciate the opportunity to be here and present to all of you this morning.

Well, California consumer rights are certainly important. There can be little debate that the CCPA does, in fact, place a significant burden on businesses doing -- conducting business in the State of California. In addition to this high cost, confusion and lack of clarity in the original language of the CCPA and -- which carries over into some of the proposed Attorney General regulations adds a further burden to companies who want to truly comply with the CCPA.

I will focus very briefly on four provisions that I think should be modified, some slightly, some in more detail as well as one additional regulations which I believe should be added.

First of all, a number of sections use the word "accessibility" as a requirement under the CCPA, talking about accessibility to consumers with

OLA 13-1

disabilities. The question becomes what does accessible mean in the context of the CCPA? Is it something more in line with the American Disabilities Act, the ADA, or is it a different standard? Given the great uncertainty that exists in the court system today with respect to website ADA compliance, I believe some further definition of this term within the CCPA should be considered. Rather than leaving businesses trying to guess what compliance means, I think it would be more helpful to spell it out.

OLA 13-1 cont

Secondly, I think that there is an easier, more clean way to streamline requests -- methods for submitting requests. If you look at proposed Regulation 999.312, Sections A and B, there are two different standards for submitting either a request to know, or a request to delete. As you know, 312A requires a toll-free number plus a web form, while Section B offers several alternatives including a toll-free number, web form, and several other standards.

OLA 13-2

I will be submitting written comments which have more, sort of, robust language, but my suggestion to the group is rather than having two different standards, combine them into one and provide two opportunities: One, I'll call a tech savvy

opportunity, whether that be an online form, an email address; and for the non-tech savvy consumer, they have the option of a toll-free number, submitting a form in-person, or providing a letter.

Now requiring businesses to choose one from each of these categories still provides two methods to make these requests, but it clarifies and, again, we're not adding -- we're taking burdens way from these companies that are truly trying to comply with this. And again, this was mentioned briefly by Speaker No. 11, so I won't spend much more time on that.

OLA 13-2 cont

The third thing, I believe that proposed regulations 313A, which requires a business to confirm receipt within ten days. I believe that language can be very easily adapted to say, ten business days. The reason being is we all know with holidays and especially this time of year, you can submit a request on the Wednesday before Thanksgiving, and a business may not see it until the following Monday, thereby providing them with literally five business days to comply. I think that that -- adding the term "business" maintains the integrity behind that regulation without adding increased pressure on compliance.

OLA 13-3

The last language issue that I'll cite to you is the 15 day requirement in 999.315 E and F, which really detail a very challenging timeline for businesses when they receive an opt-out request. Trying to turnaround an opt-out request maybe very challenging particularly with a 90-day look back. And given that there's a 90-day look back, I don't see the need to have 15 days as opposed to the normal 45 plus 45 day standards which appear in other sections of the CCPA. At a minimum for large businesses, 15 plus 15 should be considered.

OLA 13-4

Lastly -- this will be my last point. I believe an additional regulation should be added to the Attorney General regs that really clarify that the enforcement action lies with, and only with, the California Attorney General with respect to privacy violations. There is a real concern in the business community that you will see folks trying to use pocket-type claims, private Attorney General actions, and/or the Unruh Act to expand the CCPA and its privacy violations beyond which it is intended to be by the legislature. I believe that that language -- adding this language to the regs will bring much needed assurances to business leaders that the CCPA will not lead to a land slide of ill-advised lawsuits

OLA 13-5

in this action.

Thank you very much for your time.

MR. AKERS: Thank you. Speaker No. 14, please.

MS. MCMILLAN: Good morning. My name is Leigh McMillan. It's L-E-I-G-H, M-C-M-I-L-L-A-N, and I am the CEO of Whitepages, which started 23 years ago as an online directory.

Today Whitepages is used by more than 30 million consumers and small businesses every month to meet a number of needs, chief among them is fraud prevention, scam call detection, and personal safety. We meet these needs by aggregating data from diverse sources and making it fully transparent and easy to access and navigate. We also strive to make it easy for individuals to request removal of their information and are constantly working to improve this process which involves matching data points across multiple sources and verifying requestor's information with limited data point as was highlighted by previous speakers.

I'm here today, first, to voice support for the goals and spirit of CCPA. We believe that individuals have the right to know how personal information they provide to companies is used and

should have reasonably and meaningful controls over how it's collected, used, and shared.

Whitepages extensive experience with data management and fraud prevention at scale informs the second purpose for my limited comments today, which is to speak to the practicalities and potential for fraudulent actions associated with the notice at collection of personal information.

Section 999.305 appears to say that short of securing after the fact written attestation from originators of the data, businesses that sell or make available personal information not collected directly from consumers must notify them of its existence and the right to opt-out. This notification requirement will flood consumers with potentially confusing notifications from legitimate companies with legitimate services. As evidenced with the misunderstandings of direct marketing requirements under the GDPR, that led to a flood of opt-in requests prior to May of 2018. The request will -- the result will be consumer fatigue and irritation all while creating a ripe environment for fraud.

OLA 14-1

Fraudsters adept at impersonating legitimate companies will take advantage of the flood of notifications that use calls to action that

consumers expect to see whether clicking on a link or supplying personal data to entice individuals to provide the exact information that CCPA is trying to protect.

The notice of opt-out from sales in the form of a "please do not sell my personal information" button to be prominently displayed on websites was determined by the legislature to be clear and sufficient. Moreover, the Data Broker Registry, with its current very broad definition of what constitutes a data broker, will allow consumers to verify, find, and easily select those entities from which they wish to opt-out of -- from.

OLA 14-1 cont

Likewise, requests for information associated with households or frequently shared identifiers, such as street address or IP address, raise substantial privacy concerns. These requests can easily be exploited by identity thieves and abusers.

James, Paver, a PhD student in Oxford provides a real world example of this vulnerability. While sitting at an airport gate, he and his fiancé began an experiment to see what data could be extracted from companies under GDPR. Over a two month period, Paver sent out 150 GDPR requests in his

fiancé's name asking for all data associated with her. Twenty-four percent of the respondents provided all files associated with his fiancé based on just two pieces of data, an email address and a phone number.

OLA 14-1 cont

To help reduce these risks, we applaud requiring agents operating on a consumer's behalf to register with the Attorney General's office so companies can better verify third-party requests. We also strongly encourage a risk based approach to request verification that gives businesses the flexibility to adopt verification solutions that are contextually relevant to their business and the data being requested, and not only disincentivize fraudulent requests but prevent them.

OLA 14-2

As noted by a prior speaker, consumers win if businesses are successful at implementing CCPA. We believe that privacy reform will bring significant benefits to consumers, but the details are critically important. We hope the concerns expressed here will be helpful to you and plan to submit additional written testimony.

Thank you for the opportunity to share from our perspective and experience.

MR. AKERS: Thank you. We've been going for about an hour. Let's plan to take a

ten-minute break at this point to give our court reporter a chance to rest his fingers. It is currently 11:03. Let's come back at 11:13. Thanks all.

(Off the record.)

MR. MCELROY: Good morning.

MR. AKERS: Good morning.

MR. MCELROY: My name is Scott McElroy. That's spelled S-C-O-T-T, M-C-E-L-R-O-Y. I'm representing a company called Paylidify. We're a multinational payment -- merchant payment processor.

So we're looking for just a few clarifications. So first off, it would be very helpful is specifics were provided on exactly how a business is to actually verify a verifiable consumer request. As a follow-up, it would be helpful if examples were provided of data elements of businesses required to collect from a consumer in order to confirm that their request to opt-out is actually verifiable. Next up, would a business that meets the CCPA threshold criteria be in violation if that business does not have a link on their website to allow a consumer to opt-out of data collection mechanisms? And finally, how many days does the business have to complete on opt-out request?

OLA 15-1

OLA 15-2

OLA 15-3

That's it.

MR. AKERS: Thank you, sir.

MR. MCELROY: Thank you.

MR. AKERS: All right. Speaker No. 16, please.

Good morning.

MR. HOSSAIN: Good morning. My name is Roman Hossain. That's R-O-M-A-N, last name, H-O-S-S-A-I-N. I represent a company called Review Squash. We are a small business digital marketing agency, and my comments are both sides -- both from the business side and the consumer side. So this will -- this will add to also Speaker No. 11's IP address only issue.

According to law firm Perkins Coie and a recent Microsoft webinar on CCPA, 140 visits a day by California consumers on a website which collects cookies and other information would cause a small business to meet the threshold of 50,000 records and be subject to CCPA in a year. This now opens CCPA enforcement of small businesses such as doctors, lawyers, CPA's, plumbers, AC repairmen, beauty suppliers, and hundreds more. And these businesses will unlikely have the technical resources to comply with CCPA. So this -- the question is was this the

OLA 16-1

intent of the law to apply to such small businesses, many with revenues of less than a million dollars a year?

For example, one of the things that our agency does is create Facebook ad campaigns for these small businesses. Well, the way the Facebook data works and by installing a Google pixel code onto their website, it opens up a database of all of Facebook's potential consumers. And as a result, 90 percent of my small businesses run Facebook campaigns. So theoretically, they would be subject to the CCPA because they've got access to well over 50,000 records on their advertising campaign. And on any given advertising campaign, we collect anywhere between 50 to 100,000 impressions for less than $500 on an advertising campaign.

OLA 16-1

So the question is is there going to be some clarification as to what a consumer record is? And the IP address only issue is one issue, but a cookie issue and a Google pixel -- or -- or the Facebook pixel issue is a whole other issue as to what records are collected.

Secondarily, I'd like to bring up the fact of on a consumer point, in going to the current AG's website, it's unclear where someone would even go

OLA 16-2

to report a violation. And so, I'm not sure if that's something that is going to be addressed in 2020, but at the current state, there's obviously numerous sections on the AG's website for numerous other business complaints, and there is a general business complaint section. But it would help if that was clarified, or if there was a specific button for that.

OLA 16-2 cont

The next issue is what will the AG's enforcement actions look like for small businesses that violate CCPA unknowingly? And although there is been some guidelines of a letter being sent, and there is about seven days to comply, and then a fine of $2,500 and then another fine of $7,500. But who are the contacts? Is there any sort of mediation? Or if the action is corrected, or if the business shows that action as being in progress of being corrected, what are kind of the repercussions of such?

OLA 16-3

And those are all my comments.

MR. AKERS: Thank you. Speaker No. 17, please. Speaker No. 17. Okay. No seeing 17. Moving on to 18. 19?

Good morning.

MR. GRIMALDI: Good morning. Thank you all for doing this. I appreciated the opportunity to be here earlier in the year for your first session and

found it informative hearing all the comments, and I'm glad to be back. So thank you.

My name is Dave Grimaldi, and I'm Executive Vice President of the Interactive Advertising Bureau. Founded in 1996, we represent over 650 leading media and technology companies that are responsible for selling, delivering, and optimizing digital advertising campaigns. Working with our member companies, the IAB develops technical standards and best practices and fields critical research on interactive advertising while also educating brands, agencies, and the wider business community on the importance of digital marketing.

We are committed to professional development and elevating the knowledge, skills, and expertise, and diversity of the workforce across the industry. IAB strongly supports the principles of the California Consumer Privacy Act, namely transparency, control, accountability, and choice. As the CCPA states, "California consumers should be able to exercise control over their personal information, and they want to be certain that there are safeguards against misuse of their personal information." And we agree. Our cross industry development of the Digital Advertising Alliance, or the DAA, was created

precisely to address those core concepts and has gained widespread acclaim from government and public interest groups alike.

Our commitment to these principles is also visible through our ongoing work to help industry comply with CCPA through the IAB CCPA Compliance Framework for publishers and technology companies. This compliance framework is intended to provide companies with the technical and contractual tools to help them fulfill consumer opt-out requests, and ultimately our goal with this framework is to increase compliance with CCPA and IAB's over 600 member companies.

But as the Attorney General's regulatory impact assessment highlights, the cost of complying with CCPA have been, and will continue to be, significant. So it's crucial that the Attorney General's office work diligently to further the purpose of CCPA without creating unnecessary compliance costs for businesses that will limit product and service availability for California consumers. IAB will be submitting detailed written comments to the Attorney General's office this week, but today I'll like to highlight just a few issues that we feel could provide guidance and clarification

to businesses in the media and marketing industries as they work to comply with CCPA.

First, IAB asked the Attorney General to clarify that using personal information received from a person or entity to service another person or entity could constitute a permissible quote/unquote "business purpose" under CCPA. So long as such use is for the benefit of the entity providing the information and is set forth in the required contract between the business and the service provider and is otherwise consistent with the requirements of CCPA. Such an acknowledgement would better align the regulations with the text of CCPA which explicitly permits disclosures to service providers for a list of enumerated business purposes under the statute. It would also better align with CCPA's definition of business purpose which includes both a business' or a service provider's operational purposes or other notified purposes.

OLA 19-1

Second, IAB asked the AG to allow companies the option of honoring browser settings or including a 'do not sell my personal information' link on its website. The proposed regulations state that "browser plug-ins and other mechanisms must constitute a valid request to opt-out by the consumer." That was

OLA 19-2

not included in the text of CCPA and could risk undermining consumer choice. We believe it's important for consumers to have granular controls over the selling of their personal information, and the current proposed regulations risk limiting that control absent further clarification and limitations on such mechanisms.

OLA 19-2 cont

I appreciate the opportunity to be able to speak with you today. You will see our filling by Friday. And thank you again for holding this forum.

MR. AKERS: Thank you. Speaker No. 20, please.

Good morning.

MR. KIM: Good morning. My name is Bo Kim, Senior Privacy Counsel at Perkins Coie and Counsel for the California Chamber of Commerce. Thank you for the hearing today.

Businesses want to comply with the CCPA. Significant investments have been made by industry to comply with the CCPA as written. For these reasons, we would suggest that an enforcement based upon the regulations be delayed until January 2021 to give businesses an opportunity to conform to the regulations.

The California Chamber will be

submitting detailed comments later this week. Some highlights of those comments are as follows with other areas to follow in the write-up.

Beyond the effective date, the overarching concerns center around the fact that draft regulations go substantially beyond CCPA requirements in a number of respects that will be detailed in our letter. A few salient examples are the following:

First, proposed Section 315 regarding opt-outs: The regulations regarding tech technological mechanisms that would communicate a consumers intent to opt-out of sale under the CCPA lack clarity. It is unclear was businesses would be required to do should such mechanisms be developed. It must be assured that consumers actually intended to exercise the right to opt-out of sale under the CCPA. We are concerned that mechanisms may be developed that may not, in fact, reflect user choice. Furthermore, there is no industry accepted technical standard regarding opt-out via a browser mechanism. The requirement to notify all third-parties to whom a business has sold personal information can be tremendously burdensome. It may not be feasible considering the broad definition of sale under the CCPA. Given the breadth of the CCPA definition of

OLA 20-1

OLA 20-2

sale under Section 1798.140 T, it may be difficult for companies to identify parties that may be considered part of an exchange for valuable consideration where they lack privity or otherwise. Businesses may not have the ability to contract parties -- I'm sorry -- contact parties to whom data was made available for valuable consideration as maybe construed by the AG's office in connection with Section 1798.120. Also the requirement to opt-out users within 15 days of the request under proposed Section 315E shortens the time for the businesses to respond to opt-out requests that exist in the CCPA now.

OLA 20-2 cont

OLA 20-3

Second, proposed Sections 307 and 337 regarding financial incentives: The requirement to give notice of financial incentives for every incentive contained in proposed Section 307 is extremely burdensome and onerous. Just imagine the impracticality of a grocery store that wants to provide daily or weekly coupons to valued loyalty customers having to give notice of privacy for every offering. Moreover, as far as proposed Section 337, the vast majority of companies impacted by the CCPA utilize technology but are not tech companies. As such, there is no particular value of data allocated on any existing balance sheet or for public companies

OLA 20-4

10K or 10Q filing. The requirement to create a data valuation under Section 337 would be artificial in the sense that value calculations for data are not the way businesses operate, and the proposed calculations exceed the statutory construct.

OLA 20-4 cont

Third, proposed Section 313 regarding responding to requests to know and requests to delete: Here again, there are areas where the proposed regulations exceeded scope of the CCPA. This includes the fact that unverifiable requests to delete should not be treated as sale opt-outs because adding unverified requests undermines the legislation which clearly provides only verified consumer requests the ability to ask for deletion as previously mentioned by other speakers. It also changes the consumers intent, increases cost, and exacerbates difficulties with deleting data from archives or backups. The Chamber also has comments on the service provider language in Section 314 and the definitions contained in Section 301 that will be in our written comments. For the sake of time, I will not repeat them here.

OLA 20-5

Thank you very much.

MR. AKERS: Thank you. Speaker No. 21, please. Good morning.

MR. RECHT: Good morning to you.

Philip Recht of the Mayer Brown Law Firm. Our firm represents a coalition of companies that provide background reports, fraud detection, and other people search services. These services are widely used by an array of California and other law enforcement, government agencies, businesses, individuals, and families alike. The companies do not collect PI directly from consumers, but instead collect it from a host of public and other third-party sources. The PI they collect is almost always already in the public domain, and the revenue from these companies derives almost exclusively from the sale of reports containing this PI. These companies strongly support the CCPA. In fact, they have been pioneers in the use and the provision of opt-out rights and a lot of the other rights that are the CCPA on a voluntary basis for years and years and years. However, they have concerns with three provisions in the proposed regulations.

The first item of concern is the notice of collection provision that has been addressed by some other speakers. This, from our vantage point, would relieve companies like ours of the need to provide what we call the "pre-collection notice," the notice required at or before the collection of PI.

OLA 21-1

Instead it would require these companies to do one of two things: Either provide direct notice before they sell the PI of a consumer, or instead obtain an attestation from the original source of the PI that that source provided a direct notice to the consumer.

This proposal is problematic in any number of ways. First and foremost, no matter how well intended, an administrative regulation simply cannot override or eliminate a clear statutory requirement such as the need to provide notice at or before collection. Even if it could, the alternative compliance options are simply unworkable for our companies. The direct notice option doesn't work because in many instances the PI that we collect doesn't even contain contact information. And when it does, that information often is incorrect or unusable. Other speakers are going to come after me and explain other problems with this as well.

OLA 21-1 cont

The attestation option doesn't work because in the vast majority of cases, almost all cases, our PI sources themselves are indirect sources of the PI, and they cannot provide direct notice. And even if they could, they will not agree to attest to anything in compliance with the law and expose themselves to new legal liabilities.

Since neither option is workable for us, the upshot of this proposal is it makes it impossible for us to comply with the CCPA, and it effectively puts us out of business in the State of California, at least with respect to California consumers. And, of course, we all know, the law will never tolerate such a harsh result when there are reasonable alternatives on this topic. And the good news here is there is a very reasonable alternative which is to allow these companies to provide the pre-collection notice on their internet homepages. It's the only practicable way for them to do it. It's consistent with the way CCPA mandates opt-out and other notices. This is how consumers search for online company disclosures. It's consistent with the approach of the new Data Broker Registry that you just heard mentioned of a moment ago. And this registry was developed to address the exact concern that I think underlines your proposal here. It's consistent with the new California Privacy Rights Act -- the new initiative, which specifically allows these companies to provide the pre-collection notice on their internet homepages. And lastly, it's consistent with the fact that the collection and sale of public domain data is constitutionally protected commercial speech. And as

OLA 21-1 cont

we know that kind of speech can only be abridged if there's a compelling reason to do so, and clearly a proposal that would outlaw these activities, when less onerous alternatives exist, could never meet the standard.

So for all these reasons, we would request that this Section 305D be amended to allow companies to provide the pre-collection notice on their internet homepages.

I have two other issues I'd like to address, but if it's possible, I think I'll wait till the end, and it'll take two or three minutes. I don't want to go over my time.

Thank you very much.

MR. AKERS: Thank you. Speaker No. 22.

MR. COHEN: I would just like to thank -- say that I very much appreciate the opportunity to address the public though this open forum today, so thank you very much to the panel.

My name is Ross Cohen, and I co-founded our company, BeenVerified, nearly 14 years ago with the mission of bringing publicly available data to the average and everyday consumer. Back then during the nascency of the internet, we saw that in order for the internet to grow and evolve, there would need to be a

OLA 21-1 cont

certain level of trust, comfort, and confidence that deeper level of connections could be made whether in the context of dating, person-to person commerce, neighborhood relationships, and even the simple right to better know who may be driving my daughter's carpool.

Over these last 14 years, we've received emails and letters from our countless families and long lost friends that have successfully reconnected using our people search engine. We witnessed myriad moving reunions such as the story of an NFL linebacker named Ahmad Thomas who used to locate and reunite his biological parents. With just their full names to go on, this once separated family found each other and formed a lasting bond that was over two decades in the making. This is just one public example of so many who have experienced this type of incredible reunion.

From BeenVerified's inception, we've helped millions of consumers and have tried to balance the responsibility of third-party public data we collect with the privacy of individuals. We've given individuals the right and the ability to opt-out their data for the last ten years using a clear link right from our homepage. However, I stand here to cite a

number of issues as well as a giant problem of unintended consequences that come along with the pre-collection notice requirement under CCPA.

First, the ability for companies like ours to provide direct notification to consumers with whom we lack a direct relationship is impractical, and at or before the point of collection because we lack any useable contact information at this time.

OLA 22-1

Secondly, even if companies were somehow to be able to provide consumers with direct notice at or before collection, it becomes an enormous problem for many reasons. Such notices would entail us contacting literally tens of millions of California residents with whom we have no direct relationship. This would be akin to the spam emails and robocalls that consumers are not only fed up with, but also opens the door to identity theft scammers to pretend that they are one of the thousands of legitimate companies who will need to provide pre-collection notice when instead these opportunities -- these opportunists will use the name of CCPA notice provision as a tool to further scam and request Social Security numbers and other private data this law was intended to protect.

OLA 22-2

Look no further than the GDPR notice

provision similar to CCPA's, and the countless victims who have received spam emails from scammers posing and companies such as Airbnb, in the name of privacy under GDPR requesting private information. In one such case, outlined in an article by The Sun, a UK publication, an elderly man said he had 4,000 pounds robbed from his account after a scam GDPR email fooled him into offering up his personal info. And stories like this are not an isolated incident either. I urge each and every one of you here to Google GDPR email scams, and you will clearly see that these sometimes even good intentions could have very unintended consequences.

OLA 22-2 cont

The direct notice requirement could create a breeding ground in California for spammer and scammers to extract the very data that we're trying to protect. In fact, at BeenVerified, we also collect user generated robocall phone complaints and just recently concluded an in depth study in part with Forbes.com on the rise of Social Security scam robocalls. This phone scam was by far the most common phone scam this year, accounting for nearly 10 percent of all fraudulent calls according to our nationwide analysis of more than 200,000 spam call reports. Victims wire money, send gift cards, or surrender

personal information to scammers. Last year, this type of fraud cost Americans $19 million according to the Federal Trade Commission. Were you to require direct notice to all Californians whose PI has been collected, this will actually open the door and give scammers exactly the next opportunity to perpetuate their next attacks.

For these reasons, we are confident that the answer to privacy protection surely cannot be sending out millions upon millions of emails or postcards from hundreds or thousands of companies. But rather should be done through both the California Data Broker Registry as clearly and conspicuously on our homepages of our companies. And we've already been offering opt-out requests for over the past ten years.

OLA 22-2 cont

I appreciate your time.

MR. AKERS: Thank you. Speaker No. 23, please. Good morning.

MR. MATTHES: Thank you for the opportunity to speak to you today. I'm Jason Matthes. I'm the General Counsel of Spokeo, and we're a member of the People Search Services Coalition as well. Like other companies that have testified previously, Spokeo uses publicly available information to enable millions

of consumers each month to connect with others, reunite, long lost friends and family and relatives, to protect themselves and their families from harm and scams. We also help businesses fight fraud. And lastly, we help law enforcement to find fugitives, suspects, and witnesses. As I said we do this all with publicly available data. Examples of type of data that we collect are Whitepage phone directory data; voluntary survey -- marketing survey results; and public social media profiles.

I'm here to talk about three aspects of the regulations that are unworkable for, not only businesses similar to Spokeo, but many other businesses. Many of the speakers previously have talked about Section 305D, which would require for businesses that don't have a direct relationship with consumers to either provide direct notice at the time of sale of information or alternatively obtain the attestation. As other speakers have said whether direct notice is required at the time of collection as the statute actually requires, or whether this alternate scheme is adopted that enables notification at the time of sale. In our case, direct notice is simply not possible for many of the reasons that have been previously testified to and also would create a

OLA 23-1

very bad result for consumers and create opportunities for scams.

The attestation is likely unworkable for our companies as was previously testified. The data that we collect being publicly available often comes from aggregators themselves who could not provide an attestation that notice was given. Also the sources from which we obtain the data may have actually collected it before CCPA comes into effect, in which case, how could they provide an attestation around giving a disclosure to consumers that, frankly, was not required at the time that they collected it?

OLA 23-1 cont

The solution that we would suggest is consistent with what you've heard today. That is to allow notice to be given to consumers via the Data Broker Registry and likewise by conspicuous notice.

The second regulations that I'd like to discuss today is 315 F which requires notification of opt-out downstream to those to whom data has been sold within the last 90 days. Members of our coalition and likely other companies have resale relationships -- reseller relationships which is not a prohibited commercial arrangement under any statutory scheme whatsoever. The regulation -- the proposed regulation would require us to breach these already existing

OLA 23-2

relationships -- to breach these contracts and notify downstream recipients that they're not going to be able to exercise contractual rights that they've already acquired. So it -- the proposed regulation effectively, you know, walks companies into a scenario where they actually have to breach contracts that are already entered into. Furthermore, this downstream notification would impose significant cost to the point that it's tantamount to prohibiting resale relationships. It's very possible that those receiving data downstream are not of the size or of the scope that are regulated by CCPA. Therefore, upon receipt of a notification of an opt-out, they may not have a mechanism in place to actually address handling no longer being able to resell that data. So for those reasons, the regulation of -- proposed regulations 315 F, and likely -- likewise unworkable.

OLA 23-2 cont

The final regulations that I'd like to discuss is 317 G which singles out companies who process more than five million records per year to publish public statistics about CCPA activities. First, I'd point out that the -- what needs to be reported on is ambiguous in and of itself. I'm not sure -- there is no definition in the regulation about how companies are to determine whether they've

OLA 23-3

complied, in whole or in part, with CCPA requests. I don't really understand what a complying in part with the CCPA request would actually be. So it makes reporting on these statistics very difficult. But more importantly, the -- there's -- as many others have testified, it's a significant investment for businesses to adopt CCPA compliance to get to the standard of CCPA compliance.

OLA 23-3 cont

Like others, Spokeo supports the CCPA. The right to opt-out, we've been doing it for many years as well. But we should not compound an already significant investment with a further burden that's actually not in the statute.

Thank you very much.

MR. AKERS: Thank you. Speaker No. 24, please.

MR. LEVINE: Good morning. You've got a tag team for a little bit of humor.

MR. AKERS: Welcome.

MR. LEVINE: I'm David Levine This is my colleague, Kevin Walsh. We're principals of Groom Law Group in Washington, D.C. We're a law firm focused on employee benefits and benefits programs. We work with employers and service providers.

Today you've heard a lot about credit

unions and other organizations. We're here to talk, like one of the earlier speakers, about the employment universe that's caught up in CCPA.

We're here to testify on behalf of The SPARK Institute, which is a provider to a wide range of retirement plans and other benefit programs. It represents over a hundred million 401k accounts, so a large proportion of the U.S. population with assets that conservatively are north of $10 trillion that are impacted by CCPA. While we appreciate greatly the efforts that have been taken with the regulations at this point, we're here to testify about the need for some more clarification especially in light of enactment of AB25 at this point.

We recognize that the regulations came out right before AB25 and don't integrate the two. But we think that given, as the prior speaker mentioned this morning, that employers have notification obligations, we need some urgent guidance and clarification to make this work because the employment space is very different especially in benefits. It's not just this typical consumer type of service provider. Here, you have an employer and their people, and there's many differently levels that operate differently than your normal business to

consumer environment. As a result, employers have a big regulatory burden. Do they carry the responsibility for notification? Do other people do? Who handles it? And so, employers are really struggling.

So we have seven sort of key ideas, and Kevin's going to walk them through.

MR. WALSH: Yeah. So we -- we suggest kind of seven areas of clarifying guidance, and I'm going to race through them because we've got five minutes and there's two speakers.

So first, I mean, really the key here is we would love a model employer-employee disclosure to be provided as part of final regulations. It would make it easy. AB25 sunsets after a year in its current form. If there is not a model, I mean, it's a lot of compliance costs for not a lot of return. OLA 24-1

Second, and we really ask and recommend that guidance define benefits broadly for purposes of AB25. So when I think about benefits, I think retirement -- I think health. But more recently, we've been more and more employers wanting to do things like help employees pay their student loans. So if benefits is defined narrowly, we risk kind of providing access for kind of vital services or things OLA 24-2

that really could help employee populations out.

Third, we ask and recommend that guidance -- that personal information -- you know, that it stays within the scope of AB25, whether it's gathered by the employer, whether it's gathered by a service provider, whether it's used by the employer, whether it's used by a service provider in the context of benefits. So it shouldn't matter who's getting it -- who's using it for AB25.

MR. LEVINE: A lot of this is outsourced, which is why we raise that point.

MR. WALSH: Fourth, and this is kind of a pretty basic one, and I think if benefits people had been writing CCPA with be this is would have been in there. But when we're thinking about benefits, we can't just think about employees and employers. We need to include beneficiaries -- so the spouse. They should fit within AB25, even though the text of it doesn't mention beneficiary because otherwise it doesn't hang together.

Now fifth, we recommend that a notice provided to an employee satisfy the disclosure requirement for a notice provided to a dependent -- to a spouse because you're going to need information about beneficiaries and spouses to operate these

OLA 24-2 cont

OLA 24-3

OLA 24-4

OLA 24-5

plans. And that's kind of works with IRS or ERISA.

Sixth, because employers won't always have a complete data -- I mixed one up. We recommend that if a disclosure provided by the employer, that it satisfies the disclosure requirement for any service provider that might interact with the employee or beneficiary directly.

And then last, the business uses in CCPA -- they provided seven examples of business uses, and the regulatory community is kind of hung up on which of those seven uses they fit under -- that benefits could be its own business use, just make that clear. This would be helpful. I mean, I think everyone wants to see benefits programs succeed. There is no reason why California should have worse benefits than anyone else.

So those are the things we'd love to see.

MR. LEVINE: So putting these things together, I think we appreciate the opportunity to bring these up. We think these are clarifications. We recognize that that things sunset at the end of next year, and we'll have to see where they land, and we can't predict. But these types of items will make it easier because right now, employers are saying how

OLA 24-5 cont

OLA 24-6

OLA 24-7

do we put this square peg of, like, the CCPA sort of standard framework into an employment relationship especially in benefits, and they're having trouble. And who can handle the notices is a huge challenge. We work at SPARK with service providers who are saying, are we supposed do it -- and employers, are we supposed to do it?

If we can have something that allows us a framework to say someone can do it. As Kevin said, this is how other regulators on the federal side do it, so that's why we recommend it.

And thank you for your time.

MR. WALSH: Thank you very much.

MR. AKERS: Thank you. Speaker No. 25. Number 25. Okay. Is there a No. 26?

MR. GARTHWAITE: Good morning.

MR. AKERS: Good morning.

MR. GARTHWAITE: My name is Field Garthwaite. I'm the Co-founder and CEO of a company, IRIS.TV, based here in LA. We work with hundreds of publishers and broadcasters, and something that I think we've heard from many of the comments this morning is that this law disproportionately effects small businesses, which I think in the context of the major tech companies that exist in this state, you can

OLA 24-7 cont

say anything under annual revenues of a billion dollars.

And it appears that the authors of this legislation did not have clear goals when it relates to the elephant in the room, which is how to do we address Google, Facebook, Amazon, and a small handful of companies -- which appear to be growing ever larger -- while other businesses are affected by these laws -- disproportionately and have teams, you know, focused on them? But, you know, the companies I just mentioned have groups larger than everyone in this room focused on these changes, and as we've noticed, you know, they're not here today.

So what I'd like to say is that there are a couple of opportunities in the legislation where there are opportunities to actually affect companies with levels of revenue of say, over ten billion, over a 100 billion, or of a certain level of market capitalization -- where the revenue received from digital transactions -- and reduce restrictions on those who're providing valuable services to consumers like many of those who have testified today of smaller size, so we reduce the effect on small businesses that focus on investing and producing -- in the case of our customers, journalism, information, and you know, the

very things that we depend on as an informed democracy. I know these are things that we all value.

Businesses such as the LA Times, for example, did not operate in the EU for months, and thousands of publishers were affected in this way following GDPR. So I hope that everyone takes note of that. The restrictions on these companies in CCPA is lesser, so I doubt that that will be the case as there's a better warning system. But that's a company that formerly was located a block way, and had many cash flow issues, and it forced a sale to a billionaire. There is been more loss of journalism jobs in this country than coal mining over the last 20 years.

So specifically in sections such as 337, calculating the value of consumer data, I just want to point out there in Article 6, that the law has an opportunity to put more onus, regulation, and transparency on the largest companies in the market and help consumers understand the distributed value that we each contribute in driving their market value. Which as of today, Facebook's market value is over half a trillion dollars at $564 billion; Google's is $890 billion. And here were standing in a room hearing companies such as small businesses -- you

OLA 26-1

know, it just seems disproportionate the way that this affects everyone.

So thank you for your time.

MR. AKERS: Thank you. Speaker No. 27, please.

UNIDENTIFIED SPEAKER: Hello everyone. And hello Ms. Blume, Ms. Akers, Ms. Kim, and Mr. Osgood. I am going to either say -- because it's so close to noon, a very late good morning or a very earlier good afternoon.

I'm going to defer to all of the speakers that have spoken representing businesses because I am a CEO and founder of a very small start-up. So I wear that hat; I also wear another hat of a consumer; and I wear on more hat as a Safe at Home program participant in the State of California. And I'm showing you the card that I have of a Safe at Home program participant, which gives me and thousands of other up and down this state, certain protections of privacy from data brokers, data mining companies, and data aggregators.

Google is not helping. I'm going to get into that in a minute. I'm trying to finish up long before the one minute poster is showing. So we know that Apple's CEO, Tim Cook, is a big advocate

OLA 26-1 cont

about privacy, but he is not dealing with the CCPA, the DOJ is.

So I'm going to briefly mention, as wearing the hats of three different entities, that I have -- when I was listening to all the speakers, I pretty much summed it up with the three C's: There's cost to comply for the businesses; there's confusion for the businesses; and there's in need of clarity and clarification for the businesses. I'm going to need that as well because I have that small start-up business hat on. And as a consumer, I became an expert in removing PII, personally identifiable information, offline that was asked to be a speaker several years ago at Digital Hollywood, a three-day event held at the Skirball Cultural Center twice at a year. It's also held in New York twice a year. But I was, just two weeks ago, the moderator because I became an expert in removing PII offline. And I figured out all of the problems, all of the hassles, all of the inconsistencies among the data brokers, data aggregators, data mining companies, which are affecting millions of consumers across the country.

But CCPA is for the folks in California. So the millions of people in California are going to experience even worse problems than I

OLA 27-1

did. So I'm here -- and I appreciate your time, and your interest, and your thoughtfulness. I'm here to tell you that the Privacy Enforcement and Protection Unit at the DOJ, they need to step up to the plate in terms of the Safe at Home program participants. I've been extremely disappointed with them, not only for their opt-out written demand form, but they're ridiculous -- and please forgive me -- directory to remove their PII offline through snail mail -- antiquated, outdated, and many of it, not all, but many of it incorrect.

So I don't know who's in charge of that specifically, at the DOJ in the Privacy Enforcement and Protection Unit because they never give any names, never provide a phone number, never really do much of anything in terms of authenticity or transparency, which is a problem when you're a Safe at Home member. And that -- so I was going to say and that means that the Privacy Enforcement and Protection Unit in San Francisco needs to connect with the Safe at Home Department in Sacramento, and also the executive office for the Secretary of State because Secretary of State is in charge of Safe at Home program.

All right. So on that note, I want to thank you, and I'm going to be done before the minute

OLA 27-1 cont

OLA 27-2

bell is off and ask you to please -- the last thing, you've got to -- you've got to deal with Google because they're -- Google is not respecting at least the Safe at Home program participants. They don't know how, and they make it impossible to provide any information for Safe at Home people to get their information removed offline. And consumers need to have control over what they -- what they want online and what they don't because I know a lot of businesses have said if they're -- they may lose their business, but people have been threatened with rape, and death, and killings because their information was put online.

OLA 27-2 cont

Thank you very much for your time and look forward to hearing from all of you very shortly.

MR. AKERS: Thank you. Speaker No. 28, please.

Good morning

DR. HENRY: Good morning. I'm Dr. Maxine Henry, and I'm the President of Cyvient. My organization is responsible for implementing and consulting services for companies in the need of governance, risk, and compliance. So essentially, we are the company that helps companies comply with the regulation.

OLA 28-1

I'm here today to speak on two sections

or two provisions of the proposed law, Section 999.313, and notable Item C5, which is the sections that deals with the denial requests. My ask here is that there be a time period specified for the denial request, if that be possible.

OLA 28-1 cont

And then the second area is Item 6, under that same section is "businesses shall use reasonable security measures when transmitting personal information to the consumer." We ask that you be specific about what "reasonable" means. Because reasonable to one company may be differently to another. And also, additional here would be to ask to provide some guidance. When your implementing aspects of the law, it would be helpful to have some information or some guidelines around particular security measures. This comes up whenever I talk to a customer. They ask what does that actually mean, and my interpretation is to provide some direction from either ISO 27001 & 2, or 27701 or either NIST 53, Revision 5. So if that be possible to provide some guidelines and some more specific language around what security measures that would be helpful.

OLA 28-2

Thank you for your time. Appreciate it.

MR. AKERS: Thank you. Speaker No. 29,

please. Do we have a Speaker No. 29?

Okay. I believe we may have exhausted our speakers. Are there -- is there anybody else who has a number to speak? Are there any speakers that would want -- who have spoken who wish a few more minutes to extend their comments?

Sir, please, come on up. And if, again, if you could keep the further comments under five minutes.

MR. RECHT: Thank you. Again, Phil Recht of the Mayer Brown Law Firm representing a coalition of people search service companies. This should only take about two minutes.

I want to address the two other issues of concern to our group. You just heard from Mr. Matthes this a while back. He addressed them from an operational standpoint. Let me try to address them from a legal standpoint.

The first one -- the first section is Section 315F. That's the section that would require the seller of personal information that receives an optout request to provide downstream notice to the buyer -- the recent buyers of that PI instructing them not to resell the PI. And then going back and informing the opting-out consumer that these tasks

OLA 21-2

have been performed. From a legal standpoint, this is problematic for two reasons. First, there is nothing in the CCPA itself, the underlying statute, that requires any similar downstream notice of consumer opt-outs, let alone imposing any limits on the resale of a consumer's PI. And for what it's worth, the same is true of the new initiative, the CPRA.

Secondly, because nothing in the CCPA prevents the resale of a consumer's PI, the proposal would, from a legal standpoint, impair the contract rights of buyers, and as we know, this violates the contract clauses of both the US and California constitutions. So for these reasons, from a legal standpoint and additionally from an operational standpoint, we ask that this provision be deleted.

OLA 21-2 cont

The last section I want to mention is Section 317G. And this is the section that requires businesses that process five million or more consumer records per year to compile data -- excuse me -- about how many consumer requests they collect, how they handle the requests -- deny or to process in part or in total -- how long it takes to do so, and then to publish that data in their privacy policies or on their websites. Again, from a legal standpoint, this is problematic. First, once again, there is nothing

OLA 21-3

in the CCPA, the underlying statute, that requires any similar data collection and publication exercise. And for data brokers in particular, the mandatory nature of this requirement conflicts with the permissive nature of the Data Broker Registry, which allows, but does not require -- but which allows listed companies to publish whatever additional data or information they want concerning their data collection practices. So again, we would, once again, ask that this requirement be removed.

OLA 21-3 cont

Thank you so much for your attention. We'll be providing detailed written comments by this Friday.

MR. AKERS: Thank you. Are there any further speakers?

Okay. Seeing none at this time, as it appears that there are no more persons present to make oral comments, I'm going to close this hearing at 12:03 p.m. on the proposed California Consumer Privacy Act regulations. Again, you're more than welcome to submit written comments. The written comments period ends on December the 6th, 2019 at 5 p.m. And written comments may be emailed to our website -- or submitted via our website or emailed to privacyregulations -- one word -- @doj.ca.gov.

On behalf of Department of Justice, thank you for your time today and participating in the rule-making process.

(Whereupon, the meeting concluded at 12:04 p.m.)

CERTIFICATE OF NOTARY PUBLIC

I, LUIS VAZQUEZ, the officer before whom the foregoing proceedings were taken, do hereby certify that any witness(es) in the foregoing proceedings, prior to testifying, were duly sworn; that the proceedings were recorded by me and thereafter reduced to typewriting by a qualified transcriptionist; that said digital audio recording of said proceedings are a true and accurate record to the best of my knowledge, skills, and ability; that I am neither counsel for, related to, nor employed by any of the parties to the action in which this was taken; and, further, that I am not a relative or employee of any counsel or attorney employed by the parties hereto, nor financially or otherwise interested in the outcome of this action.

Dated: December 12, 2019

LUIS VAZQUEZ
Notary Public in and for the
State of California

CERTIFICATE OF TRANSCRIBER

I, DONNA CAPOLONGO, do hereby certify that this transcript was prepared from the digital audio recording of the foregoing proceeding, that said transcript is a true and accurate record of the proceedings to the best of my knowledge, skills, and ability; that I am neither counsel for, related to, nor employed by any of the parties to the action in which this was taken; and, further, that I am not a relative or employee of any counsel or attorney employed by the parties hereto, nor financially or otherwise interested in the outcome of this action.

Dated: December 12, 2019

DONNA CAPOLONGO