STATE OF CALIFORNIA

DEPARTMENT OF JUSTICE

OFFICE OF THE CALIFORNIA ATTORNEY GENERAL

****

PUBLIC FORUM OF THE DEPARTMENT OF JUSTICE CALIFORNIA CONSUMER PROTECTION ACT CONSUMER PRIVACY ACTS

TRANSCRIPT OF PROCEEDINGS

Wednesday, February 13, 2019

10:27 A.M.

California State Building

2550 Mariposa Mall, Room 1036

Fresno, California

Vanessa Harskamp, RPR, CRR, CSR No. 5679

APPEARANCES

STATE OF CALIFORNIA
DEPARTMENT OF JUSTICE
OFFICE OF THE ATTORNEY GENERAL
455 Golden Gate Avenue, Suite 11000
SACRAMENTO, CALIFORNIA 94102

DEVIN MAUNEY
Deputy Attorney General
Consumer Law Section
[redacted]

LISA BOYOUNG KIM
Deputy Attorney General
Privacy Unit
[redacted]

DANIEL BERTONI
Staff Services Analyst
[redacted]

JENNIFER KING
Executive Assistant
[redacted]

FRESNO, CALIFORNIA

WEDNESDAY, FEBRUARY 13, 2019

MR. MAUNEY: Good morning. Thank you so much for your patience. It is very much appreciated. As you can tell, we -- it is very important that we hear your comments, and so we wanted to make sure that everyone has arrived, despite some travel difficulties caused by the weather.

On behalf of the California Department of Justice and Attorney General Xavier Becerra, welcome to the 6th Public Forum on the California Consumer Privacy Act.

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

Today our goal is to listen. We are not able to answer questions or respond to comments. Before we begin, we'd like to briefly introduce ourselves.

I am Devin Mauney, I'm a Deputy Attorney General with the Consumer Law Section.

MS. KIM: I am Lisa Kim, Deputy Attorney

General with the Privacy Unit. And, again, I apologize for being late. The plane had some technical difficulties.

MR. BERTONI: And I'm Dan Bertoni. I am a researcher in the Attorney General's executive office.

MR. MAUNEY: We will begin in just a moment, but we have a few process points to go over for today's forum. Each speaker will have five minutes. Please be respectful of our timekeeper and your fellow speakers here today.

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

The front row is reserved for speakers. When you come up to the microphone, it is requested, but not required, that you identify yourself when you are offering your public comment.

It would be helpful if you have a business card that you can hand to the court reporter. We welcome written comments by e-mail or mail as well.

As I mentioned before, bathrooms are out the door to the left of the security desk.

If there is any media present here today, would you mind just raising your hand to identify yourself?

So the rulemaking process is governed by the

California Administrative Procedures Act. During this process, the proposed regulations and supporting documents will be reviewed by various state agencies, including the Department of Finance and the Office of Administrative Law, or OAL.

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

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

The public hearings will take place during the formal rulemaking process, will be web-casted and videotaped. All oral and written comments received during those public hearings will be available online through our CCPA Web page. And I encourage you to stay informed throughout this process by visiting this Web page. You will find it at oag.ca.gov/privacy/CCPA.

CCPA Section 1798.185 of the Civil Code identifies specific rulemaking responsibilities of the AG. The areas are summarized here in 1 through 7. Please keep in mind these areas when you provide your public comments today.

1) Should will there be additional categories of personal information?

2) Should the definitions of unique identifiers be updated?

3) What concessions should be established to comply with state or federal law?

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

5) What type of uniform opt-out logo or button should be developed to inform consumers about the right to opt-out?

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

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

At this time, we welcome your comments.

Speakers, if you could please come down to the

front row and the first person can go right to the mic.

MS. KING: Don't be shy.

If you have a business card, you can drop it off to the court reporter.

Thank you.

MS. DENA: Good morning. My name is Ann Dena, and I represent, my company name is Raven Night. And this relates to public privacy, as well as the categories of personally identified information that are available. I have been working on a long, extensive investigation into unauthorized surveillance, and I have identified potential targets, basically from offshore individuals such as Vladimir Putin operating in conjunction with Bill Gates, and have involved technology, and I have also submitted that information online.

And I understand this meeting is basically a general meeting in regards to publicly available information. But in reality, we need to also discuss unauthorized surveillance. And I wanted that to be entered into the record, because we can talk about basically what is available online and consumer's rights, but our rights as consumers also extend to what is being done behind our backs covertly.

And I have prepared an extensive PowerPoint

presentation. I apologize, I'm nervous. Because I'm not really a public person, I'm just -- I basically do covert real -- covert investigations. So I'm not typically in front of the media or anyone in particular.

But I do intend to present this information publicly, and I wanted to have the opportunity to submit it directly in regards to this, because it's a complete package, and I know that Jerry Brown was very much aware of that package. And so I do want to present that package publicly to protect consumers.

We've been dealing with San Diego County, some individuals that have been involved in real estate transactions using methamphetamine funds and conducting unauthorized surveillance covertly. And I want that to be addressed, because those individuals have access to consumer's information subterraneanly behind our backs, and they have been utilizing it to devalue real estate. That means that every single person is vulnerable, and every single person can be covertly bankrupted.

So I would like the opportunity to present such a package, a presentation directly to Xavier Becerra or this committee.

Is that something that is possible or --

MR. MAUNEY: To the extent you have written documents that you would like to submit regarding these

rules, you can send them to the e-mail address that's there, or if you have documents that you'd like to send by the mail, you can send them to the address that's on the screen.

MS. DENA: Okay. Because basically this is -- it's nice to talk about public privacy, I mean, what we submit online. But in reality, there is much more at bay behind what is available.

For example, if individuals are able to utilize covert surveillance and capture all of our data and identify target points of individuals, that makes it much easier to steal that information.

So I do want that to be entered in as a concern for Americans and for Californians, because we stand to lose a lot by allowing information to leak out covertly. So I will send my complete presentation, including all back-up, all accompanying data, and I have found plenty of samples of photographs and things I have collected that relate to the unauthorized surveillance being conducted directly behind our backs. Thank you so much.

MR. MAUNEY: The next speaker can go ahead.

MS. LEE: One question. Who is keeping time?

MR. MAUNEY: I'm keeping time.

MS. LEE: Okay. I just wanted to know so I

don't go on forever.

So, hello. Thank you for the opportunity to comment.

My name is Jessica Lee. I am an attorney and Co-Chair of the Privacy, Security and Data Innovations Practice Group at Loeb & Loeb. I spent most of 2017 and 2018 helping clients get ready for the GDPR, and I am now counseling clients as they prepare for the CCPA.

The companies we represent care very much about respecting the privacy rights of consumers and they take the CCPA and all of their privacy regulatory obligations very seriously.

THE COURT REPORTER: Slow down, please.

MS. LEE: Excuse me? I'll try.

The first point I want to comment on is the Definition of Personal Information.

The Attorney General's Rulemaking Authority, as you pointed out, allows it to update the enumerated categories of personal date to, among other items, address obstacles in implementation, as well as privacy concerns.

Section 1798.40(o), the definition of personal information is extremely broad, and includes information that is, quote, "capable of being associated with" a particular consumer or household.

Personal information means -- sorry, excuse me.

There are two issues that could be clarified by rulemaking.

The first issue is that any information is arguably "capable" --

THE COURT REPORTER: Please slow down.

MS. LEE: -- of being associated with a particular consumer. Information should not be considered personal information until those are actually or at least reasonably associated with a specific person.

And so while we appreciate there is a desire to be broad and to capture all of the potential data elements that could be captured when an individual is present online, that definition is broad and creates significant obstacles for companies who are looking to comply and create implementation, because there is no clear standard for defining what is, quote, "capable" of being perceived as an individual.

That breadth also creates privacy challenges as it may lead to a company getting access to or deleting more information as necessary.

We recommend removing the language "capable of being associated with" from the definition. This would

retain a broad definition of personal information and a definition that would actually be inline with both domestic and international concepts of personal data.

The second issue with the definition is the inclusion of "household" in the definition. And while there might be a desire to capture shared identifiers like home telephone number and addresses or insights such as the number of devices in a home, as currently worded, this expands the definition of personal information and creates what we assume to be unintended privacy concerns.

Household is not currently defined. A household could be a family or could be strangers sharing an apartment. Without clarity as to what is meant by a household, the law could lead to information being shared to the wrong individual, for example, by scorned partners or roommates.

If the intent is to create a definition of information that is broad enough to capture data of shared data points of individuals in a household and that kind of thing, that information is covered by the examples and the concept of data that reasonably relates to a consumer.

THE COURT REPORTER: Please slow down.

MS. LEE: We recommend deleting the word

"household" from the definition of personal information and health information and adding in language to address the concept of information reasonably related to a specific individual that might be collected from shared devices.

Alternatively, we recommend defining "household" and defining recommended processes for identifying whether a consumer has the right to access all the information when that may have been collected from their household.

The second point I want to comment on is the definition of unique identifier. Rulemaking may be used to update this definition, and there are two issues that can be addressed.

The first is the inclusion of probabilistic identifiers in the definition. A unique identifier is what it sounds like, it is an identifier that gives a unique name or ID to a person or thing. All of our devices have unique IDs as an example.

Probabilistic identifiers are those that can be used to identify a consumer or a device by the degree of certainty of more probable than not based on categories of personal information. So practically, that means that anything that gives you better than a 50 percent chance of guessing personal data fields can fall

into that definition.

The fact that I've typed my notes may make it more probably that I am a lawyer, but I'm reading this from an iPad, so I might be under a certain age. This kind of data hardly seems unique. To be able to, you know, understand that someone who might have a particular shopping habit really doesn't fall into the definition of what should qualify as a unique identifier. Including this in the definition creates privacy concerns and implementation challenges.

For companies, there is little value in retaining stale probabilistic data. This information is often aggregated, if it's not updated, if someone doesn't revisit the site fulfilling probabilistic categories, that information is often deleted. It is also often upgraded to the audience so the advertisers can understand who is more ready than not to have an interest in the products.

Requiring companies to retain data that would typically either be deleted or aggregated in order to respond to consumer requests can be seriously contrary to the spirit of the law, which should really be to encourage shorter data retention periods.

Additionally, asking a company to verify that a specific individual is included in a probabilistic

data set also presents a unique challenge.

THE COURT REPORTER: Please slow down.

MS. LEE: Companies may be forced to either collect more data or retain more data.

The second concern here is a lack of incentive to pseudonymize data. In the advertising ecosystem, identifiers are often hashed to protect the security of the individual. Pseudonymization is a process of separating data collected from direct identifiers so that linkage is not possible without information that is held separately. This, again, is a privacy-protected act. As an example, the GDPR creates incentives for this act.

I'm just going to finish, so I'll skip to the end. You know, I think that we should sort of consider this concept of pseudonymization. With respect to the definition of unique identifiers, we recommend removing the reference to probabilistic identifiers from the definition, and we recommend rulemaking that recognizes that there may be categories of data that are not directly identifiable, but that do not fit within the definition of aggregate or de-identified data, and creating incentive to pseudonymize data, recognizing exceptions for data in a process that is held in a manner that is meant to sort of protect privacy will

ease the operational burden on companies for which it may not be technically feasible to identify an individual. This will also encourage more companies to process and use data in a manner that is privacy protected.

MR. MAUNEY: If I can encourage all speakers to speak as slowing as you can, just to make sure that our court reporter can get down your comments, because we want to have access to them.

MR. GORDON: Good morning. My name is Jared Gordon, and I'm an attorney for McCormick, Barstow, as well as the Co-Chair of the Internet and Privacy Law Committee of the California Lawyer's Association Business Section.

I am, however, here in my individual capacity and in my, I guess, informal capacity as a Co-Chair speaking not officially on behalf of the California Lawyer's Association, but on behalf of some of my committee members for their shared concerns on the California Consumer Privacy Act of 2018.

So each of the points I'm going to enumerate are intended to be within the nature of the potential exceptions to the CCPA, which in any stage we believe can be done on a regulated level, as opposed to requiring some changes in the statute to beyond what the

State DOJ's office is necessarily capable of doing at this point.

So first has to do with the treatment of employees in relation to the California Consumer Privacy Act, and specifically the way the consumer is defined, which is to say broadly, it certainly could encompass an employee in the context of their employment, as opposed to in the context of their being a consumer of a good or service. However, employment is not listed under the business purposes that are described later in the CCPA.

Further, given the extraordinarily large number of different federal and state recordkeeping obligations that relate to employment, to employee files, to grievances or reviews relating to employees, et cetera, including, but not limited to, those in the Labor Code and the governmental -- the Government Code of the State of California, we think it is fully consistent with both subsection 7 and subsection 8 of Section 1798.105(d) for the State AG's office to find, just on a purely regulatory level, that employees in the employment relationships can be fully excluded from the California Consumer Privacy Act, and we would urge that that be done on a regulatory level to exclude employees from consumer and definition of consumer, or purely in some other capacity, but we think it is within the

horizon.

Second, we think that business to business lists that incidentally include information about natural persons, although those natural persons are themselves consumers in other contexts, should be excluded. Those natural persons are not in that circumstance used as identifiers for themselves, they are instead contact people or representatives of the business that they are employed by or officers or owners of. And to the extent that there is personal information that might be used for them, anything from their e-mail address to their phone number to their mailing address, et cetera, if it is a business address, business phone number, a business e-mail, or otherwise representative of the business, we think it is inappropriate to include it within the consumer category.

We think it poses significant problems from a trade secret perspective for many businesses who have business-to-business lists that are important trade secrets, and potentially there are issues with the Defend Trade Secret Act as a result, if, for instance, people can start demanding that they receive information or delete information that has been collected about them, in connection. So that's the second of the four

suggested exceptions.

The third, which is a relatively broad exception, is for any interactions that might apply with the Privacy Shield. As you are almost undoubtedly aware, the United States has by both statutory law and effectively by treaty obligations for any businesses that agree to undertake the privacy issue procedure administered by the Department of Commerce, and although the interactions are far too complex to go into in a short speech, we think it is important that there be at least some recognition in the regulations that to the extent that there are inconsistent obligations that they are preempted, and we think that the State Attorney General's office should consider a complete preemption for any business that accepts U.S. Privacy Shield obligations and essentially obligates GDPR obligations.

Finally, we urge that the definition of "business" has a little additional clarity, and specifically, that the annual gross revenue descriptor within the business definition be further defined by regulation to reflect the $25 million threshold apply for at least one full financial year of a business, prior to any obligation accruing to comply with CCPA.

The reason for that is that there are, as you know, many start-ups in California, both here in Fresno,

at our level Bitwise Industries, our first space for any endeavor, hubs of technology that are building here in the Central Valley, or in the vast incubators of accommodations in Long Beach and Silicon Valley start-ups.

Now, it is frequently the case that start-ups grow at large, sometimes 10 or 20 X within one or two years. It is easy for them to get to a point where they exceed the $25 million gross revenue threshold without realizing that they have exceeded it. And because their growth is so quick, they may not be prepared or in compliance with CCPA until a significant amount of time after they reach that threshold.

My suggestion to that is there be a reasonable delay on when it applies to them so that they have time to catch up in compliance. I think a year is appropriate, and it can certainly be more, I wouldn't argue that it should be less, but some allowance should be made for some amount of comprehensive business achieved to learn that they have now reached that threshold and then to come into compliance once they have learned that they have reached that threshold.

With that, I conclude my remarks. Thank you.

MR. WHITE: Good morning. My name is Paul White. I am in-house counsel for a large corporation

that does business in 48 states, and including California. And one of my concerns with this Act is given the definition of "consumer," it really has nothing to do with consumers. It involves basically everyone in California.

And one of my concerns, the same as the last speaker about including employees and applicants in the definition of a consumer, we are trying to work this through from a practical point of view, and, obviously, we collect all sorts of information about our employees.

But then it is passed on, obviously, we have a 401(k) program, if someone goes on disability, we have worker's comp that it gets disclosed to. If somebody eventually goes on unemployment, we have to convey information to EDD. Even sometimes we get sued in class actions, we make a list of employees.

Now, from a practical point of view, if those employees are included in all this and former employees and applicants, you know, the use of the information is going to change, so now if someone quits or is going to have to have a new disclosure in our privacy area, saying we are disclosing the information to, you know, the EDD at this point. I mean, we even have, you know, we have a uniform service that we give the names of the employees to the uniform service just so their uniforms

can get cleaned and returned to the same person.

So I think it is just all sorts of impracticalities, including employees, former employees, and applicants in this, there needs to be some sort of reasonable restriction that every time someone's name comes up and is given to some third-party, we don't have to somehow change our website or our computer information or our 800 number to include a new category in disclosure. Thank you.

MS. SMITH: Good morning. I'm Betty Smith. I'm a resident in Fresno. I have a business here in Fresno, and our headquarters are here. We are a nationwide company.

And my comment is also about employees, employers, and the private data that we hold for those employees, the submission of that data to the various federal and state, city, local governments. There is so much there that we are bound as an employer to transmit.

The household data was also a concern to me as an employer, that that comment said that perhaps someone within the household that had no right to that employee's data could access it. And I would be very concerned about that. It might be improperly done.

As a business person, I transmit data for a fee, all over the United States, to the federal

government, to 401(k), to administrators of insurance. So the fee item needs to again fall into the employment and the employee consideration.

I'm also a development business, so it should be considered as this might move forward that if there is programming to be done within systems, whether it is the employer of the business, that they should be given an opportunity to define that time, and typically programming in my business is about six weeks.

Thank you very much.

MR. SHAW: I just have a brief comment to be considered. My name is Steve Shaw. I'm with the SecureData Team here in Fresno, California. And we do a lot, we are an NSP and we provide services around security and IT for our clients.

And one of the things that keeps coming up in my mind as I look through the definition of what a consumer is, also it communicates, from things that I have read from reviews of the California Consumer Privacy Act that could include devices, IP addresses such as that to count as a consumer in the State of California, and that makes it pretty complicated for us to locate how we correlate an IP address or a phone IP address or any device IP address to a consumer. That is a little difficult.

We can correlate to addresses, telephone owner, zip codes, anything to do with driver's license, anything that is publicly available information either orally, but it is really hard, if we can find that data in a customer's data that is out there in structure or structures or otherwise. But all that other information would be really hard to correlate. I don't know how that is going to be done.

So that whole definition of what is a consumer should be narrowed or redefined to the point that we could actual retrieve the data if we were requested to provide information on a particular consumer within a 45-day time frame, there has to be some way to automate that process to work, and I don't know how that could be done. I know how we do some of it, but not all of it. And that item might need to be put out there for the businesses out there who would get a request. That's my only comment, not only what a consumer is, as far as it is tied to information that could be retrieved and found out so we can tract any correlation to communications with a customer and back to a request for information on the customer. Okay.

MR. OLSON: Yeah, Brian Olson. I'm with 5 Point Cyber Security, also based in the Fresno area. A long-time IT industry, 20 years in cyber security, et

cetera, et cetera.

So I think this is a good law in a lot of ways. But I think one of the ways we could maybe strengthen it and focus it a little more is there is a lot of companies out there that have data on us that we don't know about; okay?

For instance, your car is sitting out there, and at some point it is going to be scanned by someone, a private industry person driving by looking for repo cars; okay? So they are scanning your license plate as you are sitting here. They drive through parking lots all the time.

Next thing you are driving down the road, you know there is street cameras and all this kind of stuff that are looking at you. How do you know those companies exist? Okay. How do you know that they even have your data?

I mean, there is provisions in the law that you can make a request for your data, but if you don't know who the company even is that has your data, how can you make that request?

So I'm asking that the lawmakers consider somehow some type of a mechanism where they can give the consumers a mechanism to find out the companies that have your data, because there is a lot of them out there

that we just don't know about. So just a suggestion.

MR. MAUNEY: If there's anyone who didn't complete their comments in the initial five-minute go-round, you are welcome to take a second one.

MS. LEE: I can speak more slowly now. I just had two additional points. The first on methods for opt-out requests. Rulemaking authority obviously allows rules to create to govern the submission of opt-out requests.

1798.130 requires a company to make available two or more designated methods for submitting requests. This include a 1-800 number. For many companies this presents a challenge. The cost of the 1-800 number itself might be nominal, but staffing it and facilitating, you know, receiving that information and processing the 1-800 number, you know, obviously has additional costs.

For companies that are purely web-based, and they only collect information from consumers online, creating an 1-800 number creates an unnecessary burden. If a company only collects information from online user interaction, it seems logical they could be able to provide methods for submitting requests online as well.

A company, for example, may offer an opt-out opportunity through as an icon which is the actual

device on the advertisement, as well as in the website. And so for purely web-based interactions, those two options offer the consumer multiple mechanisms to exercise their rights without creating this additional burden on the company.

We recommend rulemaking flexibility to provide more flexibility to companies to provide an opt-out mechanism in the form that is in line with the manner in which it ultimately engages the consumer.

The second point, kind of under the same header, for Sections 1798.105 and Section 1798.120 allows consumers to opt-out of the sale of their data or delete their data entirely, but it doesn't explicitly permit a business to allow a consumer a choice of what they are opting out of. If we look to a law like CAN-SPAM as an example, which allows businesses to give consumers an option opting out of maybe certain email lists or frequency of emails, but giving them more choice over actually what they are doing and what they are opting out of, the CCPA might look to a law like that to give businesses more flexibility and to give consumers more choice about what they want a company to do and not to do with their data.

And considering that the sale of data and the definition of "sale" is so broad, there might be value

to consumers who want to allow the sale, quote, "sale" as it is defined, as stated in certain purposes but not others.

So we recommend rulemaking that would allow businesses to give consumers options with respect to what they are opting out of. That could include the option to opt-out of all sales, but also the option to opt-out of certain sales as well. We think this would further the desire to give consumers more control about choice about how their data is used.

My last point on the rules regarding financial incentives. So 1798.125 prohibits businesses from discriminating against companies who have -- I'm sorry -- consumers who have exercised their rights under the law unless the value of the activity is reasonably related to the value provided to the consumer.

Many of our clients run membership sites where they have loyalty programs so the consumer can receive a benefit for providing that data. There is no real standard developed yet to assess the value of this data, and as a result, programs like memberships and loyalty-based programs may be considered to be discrimination.

And so while the law allows for "financial incentives," there is little parity around the

circumstances in which an offer would be considered a financial incentive versus discrimination.

So if the consumer rejects the financial incentive and doesn't get access to preferential pricing, as an example, or content, is that discrimination? I think these are issues that could be well clarified by rulemaking.

So thank you for the opportunity to comment, and we look forward to submitting written comments as well.

MS. KIM: So I know this silence is a bit awkward, but we want to make sure that anyone who has a desire to speak and bring comments to us however in any capacity has an opportunity to do so.

We will probably just sit in silence for the next couple of minutes and then maybe take a five-minute break and then open up again, just in case maybe something comes up that triggers your thoughts and you want to speak some more.

MR. GORDON: Once again, speaking informally, not officially, on behalf of the Internet and Privacy Law Committee of the California Lawyer's Association, which is a section separate from my earlier comments about potential exceptions that would be done on a regulatory basis, I would like to invite to the extent

that the State Attorney General's office wants any assistance from any outside attorneys to offer you the assistance of the working group that the California Lawyer's Association created specifically for privacy, and that's directly prompted entirely by CCPA, both my committee, the Internet and Privacy Law Committee Business section and the second Internet and Privacy Committee of the IT section and the Antitrust sections, of the Privacy sections, all coming together to form a working group.

We certainly are happy to provide our expertise on the law to the extent that it would be valuable to the State Attorney General's Office, we would be happy either formally or informally to provide comments or assistance in drafting in particular subsets of regulations that you may have.

And I guess you have my card, so you have my information. I know some of our other members have spoken in some of the other forums as well, so you probably can reach out to as well. Josh DeLoura, if I'm correct, spoke, I believe, in the San Francisco forum. He is my Co-Chair for the Internet and Privacy Law Committee.

But feel free to reach out if you want to any of our technical assistants, obviously, at no charge to

the State. We are happy to do that as a public service, and it's a relatively neutral third-party set of experts.

Thank you.

MS. KIM: So with that, why don't we take about a five or ten-minute break and then we will open up just for the last time.

(Recess)

MR. MAUNEY: We are going to get started again. For anyone who came in late, speakers, anyone having comments at all, you are invited to come up to the microphone.

If you can try to speak slowly and keep your comments brief, that would be appreciated, but we have more time than we have speakers so we won't hold you strictly to the five-minute rule unless many, many, many people are moved to speak now than there were before. So with that, we'll go ahead and get started again.

MS. PEPPER: Is that good? All right.

Good afternoon, and thank you for allowing me to make brief comments on the California Consumer Privacy Act.

My name is Alison Pepper, and I'm the Senior Vice-President of Government Regulations at the American Association of Advertising Agency, or 4A's for short.

Just a brief history on the 4A's. The 4A's is actually a 100-year-old organization. It's a trade association that represents advertising agencies across the country. We represent over 700 different advertising agencies, with approximately 213 of those advertising agencies being located right here in California. So California agencies represent a little over 30 percent of our memberships, so a pretty significant amount of our members.

The 4A supports the goals of the CCPA and understands the need for providing California consumers with more transparency in a recently complex and fragmented online environment. As the founding supporter of the Digital Advertising Alliance, or DAA for short, the advertising done at 4A's has been involved since 2008 in working on programs and has an established track record in working to ensure that consumers have access and choices when it comes to how their information is used online.

While supporting and recognizing the overarching goal of the CCPA, we do have some concerns of the CCPA's past, and I would just like to quickly highlight three specific concerns that the 4A's has with the CCPA's past.

The first concern is around Section

1798.115(d), and this is around explicit notice. The section prohibits a third-party from selling consumer personal information that has been sold to the third-party by a business, unless the consumer has received explicit notice and is provided an opportunity to opt-out from the business selling the data.

When a consumer chooses not to exercise his right, it is currently unclear to us on the agency side whether a third-party can really rely on the written insurance of the CCPA transferring party. It would be helpful to have clarity that recognizes the written insurance of CCPA compliance is sufficient and reasonable in this context.

The second issue is on publicly available data. Section 1798.140(o)(2) states that personal information does not include publicly available information. However, this section also states that information is not publicly available if that data is used for a purpose that is not compatible for the purpose for which the data is maintained and made available in the government records for which it is publicly maintained.

Many California public agencies already have rules and regulations about commercial use of public records. Certain public records can be used for

important reasons, from fraud prevention to auto vehicle recall. CCPA appears to introduce new uncertainties into this process by potentially creating a new category of personal information when public records are used by commercial entities outside of the purpose for which the data is maintained and made available.

It is unclear if this new determination of acceptable scope of usage would be determined by the public agency providing the record, the CCPA, or some other entity. We would ask in this scenario that some guidance be given to the companies so that they can obtain a clear understanding as to what constitutes Inscope usage before proceeding.

Then finally, my last point is around treating pseudonymized data and personal information the same, and I'm going to refer to it as "P data" for the rest of this, because it is a hard word to pronounce.

Section 1798.140(o)(1)'s definition of personal information, in combination with 1798.140(g)'s definition of "consumer" suggests that the law would treat P data in the same manner as that as a directly identified individual. P data does not include datatized but individually identifies a person.

P data is regulated in such a way that it does not attract a specific consumer without additional

information. Agencies are concerned that these definitions would require them to try to associate nonidentifiable P data, device data, with a specific person seeking to exercise their CCPA rights, thus having a potentially unintended consequence of forcing agencies to take what was previously nonidentifiable data and associate it with a specific person. Such a result would undermine consumer privacy and remove privacy protections from consumers and would appear to be contrary to some of the goals of the CCPA.

So thank you for the opportunity to speak today. The 4As appreciates the California Attorney General's office's willingness to listen to concerns associated with CCPA, and we look forward to submitting detailed written comments. Thank you.

MR. MASTRIA: Good morning. My name is Lou Mastria. I am the Executive Director of the Digital Advertising Alliance. We operate the YourAdChoices privacy program for consumers. Over the last ten years, the DAA has provided millions of people with information and choice around interest-based advertising.

The DAA strongly supports the CCPA's goals of providing Californians with better transparency and control over data. We would like to suggest a number of potential improvements to the law to better achieve

those goals from our experience in this field.

For background, the DAA was established in 2008 as a novel self-regulatory body and provider of tools for choice around interest-based advertising. We established privacy guidelines for collection of data, use, transfer of that data for advertising, and we achieved unprecedented and broad industry adoption of those standards. We have also kept pace with the rapid changes in the online industry by updating our guidelines five times over the intervening years to account for changes in technology, industry practice, as well as consumer preferences.

To ensure compliance, the DAA program is monitored and enforced across the industry by two independent organizations, including the Council of Better Business Bureaus, which together have brought more than 25 -- more than 95 public enforcement actions. Some of them are listed in this book which is made publicly available (indicating).

This also includes referrals to regulatory agencies when needed. These are some of the novel self-regulatory approaches the DAA has brought to the market. It is little wonder that the DAA's program had been called "self-regulation with teeth" by the former head of the Federal Trade Commission.

The most recognizable part of the DAA program, however, has probably been YourAdChoices icon, the small blue triangular icon that appears on ads, on websites, and in apps. By clicking on the icon, consumers can get information and control right from the ad that they are viewing. They can access the data collection and use practices of the companies that are involved in that practice, as well as being able to access an easy-to-use tool to opt-out of further data collection, use, and transfer of data for such advertising.

The YourAdChoices icon is currently displayed at a rate of a trillion times a month locally, and is helping to drive broad industry and consumer awareness of the program. In a 2016 study, DAA commissioned three in five consumers (61 percent) said that they recognized the icon and understood what it represents. Beyond the icon, the DAA's various digital properties to help consumers in this area have reached a total of 80 million unique consumers to date.

Beyond the features of the DAA program, we believe the process by which it operates and has set an important model for how stakeholders from government and industry can come together to create practical privacy solutions. We believe in collaboration and we think that policy outcomes are improved by dialogue and

engagement. So we commend you and the Attorney General's office for conducting these hearings.

In 2013, during a similar process that unfolded during the legislature's update to the California Online Privacy Protection Act, CalOPPA, after engaging with a broad range of stakeholders, the legislature decided to recognize additional mechanisms to effectuate consumer control over personal information, and that's for personal information collected across sites and across online services.

This approach provided businesses with the flexibility in implementing the privacy requirements of that law, while ensuring the consumer protections were not compromised. Since then, businesses have leveraged the DAA's choice platforms to provide this control to consumers. We ask respectfully that the AG permit consumers to continue to use these universal and centralized opt-out tools used by millions of consumers to easily and simply express their privacy preferences.

As the Attorney General's office considers the implementation process for CCPA, we want to share some of our learnings from the people who would be most affected by the law. While people want additional privacy protections, and certainly pop in mind things like identity theft and others, research also shows that

consumers see the current system as a fair value exchange and they don't want to undermine the economic framework that powers their online experiences.

A DAA study finds that consumers assign a value of nearly $1,200 a year to the ad-supported services and content available to them on computers and mobile devices. The overwhelming majority, 85 percent, said they would prefer to have those services financed via advertising through the current model than pay out-of-pocket for them, that is probably not surprising. Additionally, three-quarters, 75 percent, said they would greatly decrease their engagement with the Internet if a different model were to take its place.

Based on those consumer expectations, and the DAA's experience in managing similar efforts, we would offer three simple broad points to inform your work.

1. Different types of data demand different levels of privacy protections.

Consumers do not consider all their data to be equally sensitive, nor should the law. The DAA's guidelines are based on a common sense approach to privacy permissions that provides higher protections and greater control for more sensitive data. Data that consumers considered less sensitive is covered by an opt-out approach, while consumers must opt-in to the use

of more sensitive data, like precise location data.

At the highest level there are strict prohibitions against the use of data for certain types of eligibility purposes; for example, employment, health care, or insurance. We would encourage you to consider a similar tiered approach to data in your implementations of CCPA.

Number 2. Pseudonymous data offers stronger privacy protections than identified data. Pseudonymous data, or "P data," as was referenced earlier, like the broad categories of interest and demographic information used for advertising, are privacy protected, as administrative and technical controls are applied to not connect such data to identifiable individual consumers.

We believe businesses should be allowed to maintain the systems that separate the P data from other personal information they have on consumers, not be compelled to make this data identifiable and connected to individual accounts. Requiring businesses to connect that P identified data would, in fact, reduce privacy to consumers.

And then number 3. Build on the models that work and tools that are already in use by consumers. The YourAdChoices icon offers a ubiquitous, popular, and realtime way for consumers to access information about

data collection and use on ads, apps, mobile websites, desktop websites, as well as offering consumers a pathway to control over that data.

We humbly suggest that tools such as this, which include independent and effective enforcement, continue to be supported through CCPA just as our choice tools were inside the CalOPPA rule. For instance, rules implementing the CCPA could recognize mechanisms like the DAA choice tools as a means to provide an opt-out to the sale of pseudonymized data without requiring businesses to personalize that data in order to effectuate rights under CCPA.

In summary, the DAA strongly supports the goals of the CCPA, and we believe that our experience offers some valuable insights into the implementation process, so that the Attorney General's office can ensure that the law lives up to its promise, rather than creating a host of unintended consequences that reduce privacy and create additional risks for California residents.

Thank you for your time and we welcome any opportunity to work with your office.

MR. MAUNEY: If there are no other comments right now, we will go ahead and take another very short recess, just three to four minutes. We will come back

on in case anyone during that period has decided if they would like to make a comment, and if no one has comments at that point, we will recess for the day. So we will take another short break.

(Recess)

MR. MAUNEY: All right, everyone. We are going to go back on the record. And if there is anyone who is still planning to speak, please feel free to come forward.

The recesses always work.

MR. CAMPBELL: My name is Terry Campbell and I am with a global -- I'm a privacy officer for a global manufacturer, a DME manufacturer, Durable Medical Equipment manufacturer.

So our company falls under the business associate parts of HIPAA, so I know that that piece does not apply to us as far as the CCPA is concerned. But as a global company, we also fall under -- we have to comply with GDPR, we have to comply with Australia's regulations and Canada's regulations, so multiple privacy regulations around the world.

One of the things that I did just want to make comment on is the manpower that it has taken to implement the requirements of GDPR has been very great for our company. It's taken more manpower than we

planned. And while the intent is understood as far as privacy is concerned, a lot of times the regulations become so cumbersome that it is difficult, that the intent gets lost, and all you are doing is trying to check the box.

So I would like to just put that into the record to put under consideration as you are amending the laws and making sure that they are in place.

Thank you.

MR. MAUNEY: All right. If there is no one -- I'll say this slowly -- no one else planning to comment? All right.

Well, thank you so much for coming, and thank you very much for our court reporter for taking down all the comments. We appreciate your participation.

If you would like to submit written comments, which we would encourage you to do, please send them to the e-mail address listed here on the screen or to the postal address listed. Thank you so much.

(The forum adjourned at 11:51 a.m.)

REPORTER'S CERTIFICATION

I, Vanessa Harskamp, Certified Shorthand Reporter in and for the State of California, do hereby certify:

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

I further certify that I am not related to any of the parties to this action by blood or marriage, and that I am in no way interested in the outcome of this matter.

IN WITNESS WHEREOF, I have subscribed my name this 25th day of February, 2019.

VANESSA HARSKAMP, RPR, CRR, CCP, CSR NO. 5679