

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 ACT

Monday, January 14, 2019

10:10 a.m.

California State University, San Marcos

333 South Twin Oaks Valley Road

San Marcos, California

Reported by: Ameer D. Zaradnik, RPR, CSR No. 12430

INTRODUCTION

MS. SCHESSER: Good morning. We're going to begin.

On behalf of the California Department of Justice and Attorney General Xavier Bacerra, welcome to the second public forum on the Consumer Protection Act. We would like to thank CSU San Marcos for hosting us here today.

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

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

My name is Stacey Schesser. I'm the supervising Deputy Attorney General for the Privacy Unit.

MS. KIM: Hi, my name is Lisa Kim. I'm a Deputy Attorney General of the Press Unit.

MR. AKERS: Good morning, my name is Nick Akers. I'm a Senior Assistant Attorney General in charge of

Consumer Protection.

MS. SCHESSER: 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 the timekeeper, although we are just going to keep time here loosely. And please be respectful of your fellow speakers here today. We also have a court reporter, who will be transcribing comments, so please speak slowly and clearly.

When you registered as a speaker this morning, you should have received a speaker number. The front row is reserved for speakers, but we haven't had a tremendous amount of people registered as speakers. But what we're asking is that you come to the front row for when your speakers group is announced, and you can use the microphone in the middle of the room here.

We also welcome written comments by email or mail, and this is where you should send your written comments too. You can use the email or the mail.

The bathrooms are just out of the room and to the right.

And also before we start, are there any members of the media here today?

Okay. Thank you.

We want to give a brief overview of the rule-making process. The rule-making 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. 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. Once this informal period ends, there will be additional opportunities for the public to comment on the regulations after the proposed rules are published by the Office of Administrative Law.

We anticipate starting the formal review process, which is initiated by the filing of the Notice of Regulatory Rule Making in the fall of 2019. The public hearings that take place during the formal rule-making process will be live webcasted and videotaped. All oral and written comments received during those public hearings will also be available online through our CCPA web page.

We also encourage you to stay informed

throughout this process by visiting www.oag.ca.gov/privacy/CCPA. We will be posting updates continuously.

CCPA Section 1798.185 of the Civil Code identifies specific rule-making responsibilities of the AG. The areas are summarized here in one through seven. Please keep in mind these areas when providing your comments today.

1. Should there be additional categories of personal information?

2. Should the definition of "unique identifiers" be updated?

3. What exceptions should be established to comply with the state or federal law?

4. How should consumers 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 types 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 would like to welcome the comments from public. For those of you who have speaker numbers, please come down to the front row. And thank you.

Whoever would like to go first.

SPEAKER: Okay.

MS. SCHESSER: Let me also mention that you are not required to identify yourself during these public comments, but it's also helpful, if you have a business card, to hand one to our court reporter as well as to state who you are.

THE FOLLOWING IS A VERBATIM TRANSCRIPT OF PUBLIC
COMMENTS:

SPEAKER #1: Well, good morning. Is this on? Okay. There we go.

Well, good morning and thank you for the opportunity to provide input on the CCPA concerning its impacts on consumers and the advertising industry in particular and the digital economy in general.

My name is Chris Oswald. I'm the Senior VP of

Government Relations of the Association of National Advertisers. The ANA is the advertising industry's oldest trade association. It's membership includes nearly 2,000 companies with 235,000 brands that collectively spend or support more than \$400 billion in marketing and advertising annually. The ANA also counts amongst its membership a large number of nonprofits and charities that are affected by the CCPA, as they use data and marketing to reach donors to carry out the missions. Nearly every advertisement you see in print, online or on TV is connected in some way to ANA members' activities.

The ANA strongly supports the underlying goals of the CCPA. Privacy is an extraordinarily important value that serves meaningful protections in the marketplace. As an industry we've taken a number of steps to put these values into practice. But as we look closely at the CCPA, we're concerned that some of the aspects of the law, while well-intentioned, will have unintended consequences for consumers, businesses and advertisers that will inadvertently undermine rather than enhance consumer privacy.

We urge the AG to consider clarifying a number of provisions in the law, including the five important issues that we raise here today.

First, in Section 125 of the act, it prohibits businesses from both discriminating against consumers who have exercised their rights under the law, unless the activity is, quote, reasonably related to the value provided to the consumer. Our concern is that the "reasonably related to the value provided to the consumer" language is not defined, and there is no standard to assess its meaning.

In addition, it seems quite possible that loyalty discount programs may be considered a discriminatory practice under the Act since these programs create different price levels amongst consumers and, therefore, it may be prohibited. Consumers who make a deletion request or opt-out request will restrict the very data that allows them to participate in a loyalty program.

As a result, those consumers will automatically be treated differently. This could run afoul of the ambiguous wording in the law. Loyalty programs allow businesses to maintain and foster positive relationships with consumers. They provide consumers significant benefits in the form of lower prices and access to special offers. Accordingly, the ANA urges the AG to permit a business to offer loyalty-based discount programs that consumers value and expect without the

program constituting discrimination under the CCPA.

Second, Section 115(d) of the act prohibits a company from selling consumer personal information that it did not receive directly from the consumer unless the consumer has received, quote, explicit notice and is provided an opportunity to exercise the right to opt out of that sale.

Our concern here is that the company may have no way to directly provide explicit notice to the consumer. As such, the company must be able to verify on assurances from its data provider that the consumer received proper notice. If not, the online advertising ecosystem, which involves multiple parties that may not have direct relationships with consumers in order to deliver ads, will fall apart. These companies may not be able to provide consumers the proper notice, which would prevent them from sharing information to deliver advertising.

Accordingly, the ANA urges the AG to recognize that a written assurance of CCPA compliance is sufficient and reasonable under the circumstances.

Third, Section 105 and 120 of the CCPA allow consumers entirely to opt out of the sale of their data or delete their data, but the law does not explicitly permit a business to allow a consumer the choice to

delete or opt out regarding some but not all of their data. The law is not clear on whether circumstances can be offered -- I'm sorry. The law is not clear on whether consumers can be offered multiple choices related to their deletion or opt-out rights, even though consumers may value these additional choices.

For that reason, the ANA requests that the AG clarify that businesses may offer reasonable options to consumers to choose the types of sales they want to opt out of, the types of data they want deleted, or to completely opt out and not just have to provide an "all or nothing" option.

Fourth, Section 110(c) of the CCPA arguably requires businesses -- a business's privacy policy to disclose to the consumer, quote, specific pieces of personal information the business has collected about that consumer. Since the data differs from one consumer to another to comply with this provision, a business would need to create personalized privacy policies for each consumer that visits their website.

We don't believe that the legislature intended this outcome, as this would be incredibly burdensome and raised -- and raises the likelihood of inadvertent disclosures of specific consumer information to the wrong recipients. Also, this requirement confusingly is

found in the part of the law describing consumer access rights, which suggests that the provision is meant to cover specific consumer requests, not simply anytime the consumer looks at the privacy policy.

Thus the ANA asks the AG to clarify that a business does not need to create individualized privacy policies for each consumer to comply with the law.

Fifth and finally, Section 140(o)'s definition of "personal information" is extremely broad and includes information that is, quote, capable of being associated with or, quote, a -- sorry -- capable of being associated with, quote, a particular consumer or household, which creates tremendous ambiguity in the law.

There are three important issues here.

(A) Any data theoretically is, quote, capable of being associated with a particular consumer, which means there is no reasonable limitation on the scope of the law. Without more clarity, businesses may end up deleting or sharing more information than is necessary.

(B) The use of the term "consumer" in the CCPA arguably could include employees and employee data. When a person is acting in the marketplace on behalf of their business, that data -- the data that is captured

there is business data, not consumer data. If not corrected, this provision would allow employees to access information and potentially compromise confidential business information and inappropriately utilize deletion and opt-out rights.

(C) And, finally, the law states that information about a household is covered, although the term "household" is not defined in the law. And this could lead to information disclosures to the wrong individuals. What is a household and who's included within a household? Are roommates part of the household? Are grown children part of the household?

For these reasons, the ANA asks the AG to clarify:

1. The definition of "personal information" to ensure the term does not cover data that is just theoretically possible of being associated with the consumer or household, but is actually -- but that is actually or reasonably related to a particular consumer or household;

2. To provide clarity on the definition of "consumer" so that it does not include employee or other business data, and;

3. To clarify the definition of "household" to provide meaningful and practical guidance

to consumers and the marketplace.

Thank you for providing me the opportunity to speak today. The ANA looks forward to submitting more detailed, formal comments and working with you as the AG develops implementing rights for this important legislation. To the extent that there are needed changes in the CCPA to protect consumer privacy and other important interests that cannot be rectified in rulemaking but that are better suited for legislation, we hope the AG will make such recommendations to the California legislature. Thank you.

SPEAKER #2: Good morning. Thank you very much for giving us this opportunity. My name is John Horst, H-o-r-s-t. I'm the managing member of Xanesti Technology Services and we are a small business that offers cyber security consulting principally to the smallest businesses, starting with real estate agents, sole proprietors -- people like that.

One of my concerns is a tendency to talk past each other when we use terms like "personal information." So I want to ask to just go on record with you folks to ask that we -- that we base the work that we're going to do on definitions that are outlined

in publications that are offered by the National Institute For Standards and Technology, or NIST. This is the foundation of the work that we do in cyber security and I think it's NIST 800-122 that speaks to personally identifiable information and it actually goes into very, very great detail as to what it involves.

But I want to give you folks just sort of a layman's view of what we're dealing with here. If you put my name on a piece of paper and that's all you have, you have data. Now, that's not personally identifiable information because there may be many other people that have that name.

You can put a calendar date that happens to be my birthday in 1967; you can put that on a piece of paper and you have data, but you do not have personally identifiable information because by itself it's just a calendar day.

Put those two things together and then put a label on top of the date that says "Date of Birth," now you have personally identifiable information.

In knowledge management the textbook definition of the word "information" is data in context with other data. So if we talk about the categories in personal information, that -- I'm glad you have that up there as No. 1, because that's going to be the hardest thing to

do from a regulatory point of view is to really get to a place where we all understand what we're talking about.

To hold onto data that is reasonably possible to uniquely identify a person means that you have something in that information, there's a piece of data in that information -- which is the data in context with itself -- that will uniquely identify an individual. And in the online world today, that's usually the email address. So if you have my name and my email address, you have personally identifiable information. Because you can get data from other sources that also has my email address and you can begin to aggregate a greater and greater and greater volume of data in context about me or anybody -- or anybody else.

And so we do need to keep a tight definition in the law on "personal information." Anything that you could use to add into data from other sources to correlate with an individual is going to be personally identifiable information. And that's what you will find in NIST 800-122 special publication.

Just on an aside, about a hundred years ago, believe it or not there were three or four different definitions of a gallon. So NIST was tasked with working with industry to come to a common understanding of what a gallon was. Now, that was not a regulatory

effort, that was an industry standards effort so we agreed on what a gallon was. And here in California we have the Bureau of Weights and Measures that is a regulatory agency that builds on the work that NIST did to make sure that when we go to the gas pump, we're getting an actual gallon as defined a hundred years ago by NIST.

We're at that same place right now when it comes to cyber security and what these things mean, what is personal information, personally identifiable information. We are in the same place that we were a hundred years ago with respect to what a gallon is.

And so it's very important that we have a foundation for defining these terms that industry recognizes, and that is the National Institute for Standards and Technology's standard publication. So please keep those things in mind as you're going through this process, and I think you'll find a great deal of help.

Definition of unique identifiers: In cyber security we need to be able to track the progress of malware and viruses when they break out to the wild. And the only way to do that is with identifiers like IP address and MAC address. The IP address, the MAC address -- these are data points that cyber security

professionals, we look to map out the realm an attack might take through a system. Now, an IP address is potentially personally identifiable information if it is the IP address of a consumer's laptop or a consumer's broadband route. But it's only personally identifiable information when it is joined in context with other pieces of data that then identify that individual person.

So if you look at NIST 800-122, it speaks to IP addresses and MAC addresses as potentially -- as unique identifiers that potentially can be personally identifiable information. We need to be careful about that because cyber security professionals need to be able to work with that data. We don't need to know whose name is associated with it; we just need to work with the data that shows us or allows us to map out the path that an attack factor takes.

I think the last thing I would like to leave with you -- and I'm not entirely sure this is a regulatory matter, but I think is more of a personal amendment to the legislation -- and it has to do with liability. I'm hoping that the State will take a light touch, a light regulatory touch on this issue. And the reason why the State should take a light regulatory touch on this issue is because the State doesn't really

have skin in the game.

If a small business -- or a medium or large business -- if a business is hacked and a lawsuit is filed, it is going to be the general liability carriers -- I was kind of wondering/hoping there were people here today from the insurance industry -- it's going to the general liability carriers that are going to have to pay the attorneys, and, ultimately, they are the ones that the business is going to look to pay the judgment.

Our general liability carries are the ones that have the most skin in the game. If you're not working with the insurance industry on how to craft that, please consider reaching out to them.

What we could do with the law is we could say that, if you are breached and you are sued in court as a result of the breach and you did not have in place a cyber security plan to comply with these regulations and other applicable regulations -- a plan in place to control your cyber risks -- if you did not have that plan in place, you would be presumed liable.

This would place the insurance carriers' lawyers in position of having to prove a negative. And all three of you are lawyers; I'm sure you would appreciate that you don't want to be in that position in court of

having to prove a negative.

If the law says simply if you do not have and execute a cyber security plan -- could be a very simple plan -- but if you don't have a plan, you are presumed liable as a matter of law. And the insurance companies are going to go to their customers and they're going to say, "Look, we need to sit down. We need to get you guys into a place that works for you or we're not going to be able to right your insurance policy." That will send the wrong messages to businesses small and large about getting on board with putting together a strong cyber security plan.

But the converse should also be true. The law should provide an affirmative defense to companies big and small who do have a cyber security plan in place, and do follow. If they can make a showing in court they have the plan and they follow the plan, then that company should enjoy an affirmative defense in tort, if they were brought -- if they were sued over breach. But they should be considered presumptively liable in court if they did not have that plan.

Thank you very much.

SPEAKER #3: Hi, my name's Gary Wright. I represent two companies. Gary Wright. I represent -- I

consult two different companies for GGPR and CCPA.

To kind of piggyback on the last comments referencing NIST, keying on the business that I represent for GDPR, it would seem advantageous to rely on the NIST standards when defining categories of information, unique identifiers, et cetera, in addition consider the ISO series as well. Because when you're in a company that has to comply with both CCPA and GDPR, it would be more advantageous if definitions are exactly the same across both realms. That would make -- and including the definitions of days to comply. For example, you have 45 -- you've established 40, 45 days to get an initial response back to an individual based on one of their five rights. In GDPR we only have 30 calendar days to respond with a positive affirmation that at least we have founder data, we're taking necessary action based on the individual rights request, and if we need additional days, we will request that based on the guidelines of the GDPR.

I know there's been reluctance to reference the GDPR with CCPA, but for companies that have to comply across both boundaries, I think clear definitions and uniform definitions would be extremely advantageous.

For categories of personal information, one of my observations for the CCPA is some of the office of

the general counsel at the one particular business that I referred to, in the 1798.80 it refers to "including but not limited to" and then it lists categories. What I'm finding is some of the attorneys are just interpreting that as only the categories listed in the California Civil Code rather than many other categories that might be advantageous that may come up when an individual comes in and requests categories with their data.

I do have a reference that I had on my phone a minute ago that I can provide you that we use in the international space that we believe -- at least a data privacy officer in the one company that I represent has a very complete listing of those categories. And I'll be happy to email that reference to you. It's from a company called Enterprise Consulting Group and they've done -- it's a really nice graphic that shows all possible categories of the privacy space.

That's all I have.

MS. SCHESSER: Thank you.

So we're not -- we won't end the forum just yet because we see there's lots of people still in the audience and we want to give people an opportunity to speak, so we're just going to hang out up here for

little bit more time and give people the opportunity to come up to the mic if they'd like to.

SPEAKER #4: Since I drew number 7, I might be the next one.

My name is Timothy Blood. I'm here on behalf of myself, but also Consumer Attorneys of California and also Consumer Watchdog. I also had the privilege of being one of the people who helped draft the CCPA and testified in front of various committees in the state legislature. As I think we all know, the CCPA passed both houses of the legislature unanimously; there was not a single no vote. There is an overwhelming mandate placed on the attorney general's office to implement this law, as it was intended to fulfill the purpose of that. And you will no doubt hear from a lot of people in the business community -- some with legitimate fears, others with maybe hyped-up fears, and certainly some legitimate issues that should be worked through.

But I would urge the attorney general's office in coming up with regulations to go slowly, because we are today living in a time where, I think when we look back at the use of an aggregation of private information, we will think back on these times as quaint times, as the simple times back before it really became

an incredibly sophisticated and powerful tool. We think that the use in aggregation of private information today is powerful -- and it is -- but it is nothing like what it's going to be in the future.

So in drafting regulations, I would urge the attorney general to go slow, to interpret the statutes in a common-sense manner, to interpret them broadly, to make sure that -- that the purpose of the statute is fulfilled. One can always go back and change a regulation that is causing a problem when a problem arises. However, if a regulation is not carefully drafted and a wrongdoer or somebody who is doing something that doesn't fulfill the purpose of the statute, that person's not going to come forward to the attorney general's office later in time and say, "Hey, can we tweak this regulation? I'm getting away with something." So I would urge the attorney general to be careful.

Also, this statute is very similar to the GDPR, but it is a GDPR light in a number of different ways. Probably the biggest way, and in a way that could absolutely swallow this law up completely, is that the CCPA requires -- puts the onus on the consumer to come forward and do something -- to alert the business that they want something done or they don't want their data

used or whatever.

That means that the regulations that are drafted have to make sure that any notifications to consumers are knowing and conspicuous. And they have to be both. They can't just be conspicuous; they have to also be knowing so that the consumers fully know when they understand that when they see something what their rights are and how to act.

That is a challenge, because it is a whole wide range of people that will be ever-expanding that that notification will have to go to. And I would urge the attorney general to reach out to as many different places as possible to learn about the best way to communicate with people in a simple, comprehensive way.

We also have had the experience of going online, of clicking things or not clicking things that are now required, having no idea what we're clicking on. That is what is to be avoided in the implication of this law. So I would urge the attorney general's office to do that.

The gentleman before raised the issue of enforcement, and pleading that the attorney general act with caution in enforcing the statute. I think I can assure everybody in this room that, as far as the enforcement of this statute goes, the enforcement is

going to be exceedingly light, probably far lighter than the attorney general's office would like. The attorney general's office doesn't have the resources to fully enforce this act, particularly as it is being initially implemented. So while we should all be, of course, with enforcement and proportionality in any sort of punishment, that is not something we will have to worry about for a very long time.

Keep in mind, with this act -- this act is very unusual in California law. People -- the consumers whose rights are violated have no recourse whatsoever under the act. As a matter of fact, they specifically do not have any recourse under the act. They cannot do anything to protect themselves if their rights are violated under the act, with the exception of when a company allows for a negligently occurring data breach. But that's it.

Also, the onus of enforcement of this act falls solely on the attorney general's office. Again, fairly unique in California law. No district attorney's office can step in the shoes of the attorney general office to enforce the law, no large city attorney's offices can come in and help enforce this law. The attorney general is on its own without any additional resources. So, in that sense, I wish you all luck. But, again, I think if

you interpret things broadly, then people's real-life fears -- you know, this will take a while; this will take several years, longer, to really work through where are the real problems/where are the not existing real problems. If the attorney general errs on the side of broadly protecting consumers, broadly fulfilling the mandate of the statute, it will have plenty of opportunity without bad outcomes for businesses to tweak the regulations going forward as we go through this together.

Thank you.

MS. SCHESSER: We are going to end shortly if there's no other speakers, so if anybody else would like to come up to the microphone to offer comments, now would be a good opportunity to do that.

SPEAKER #5: Good morning. I just wanted to make this very short.

I did have a particular question with respect to forms. Various clients have asked our office to determine -- or make comments with respect to whether the attorney general intends to create some sort of standard form for the verifiable consumer requests, and they -- some of them have indicated that that would be

extremely helpful. I'm not sure if that was something that was mentioned before I arrived this morning, but their concern was that there would be difficulty in funneling the requests to the appropriate location, determining whether, in fact, the request was verifiable with respect to the consumer. And there's, of course, a concern about disclosing information to an incorrect party, someone who is seeking information about consumers that is not entitled to that information. So several of our clients have indicated that their thought is that it would be helpful to have a form established and then potentially allowing for the entity to designate a particular address or manner for submitting that form within their organization.

That's all. Thank you.

MS. SCHESSER: Okay. With that, we'd like to thank everybody for coming today and thank you for your comments. If there's anything further that you would like to share with us, please -- you can send us an email at the privacyregulations@doj.ca.gov mailbox or to the mailing address, and I can put it back on the screen if people would find that helpful.

And thank you again.

(Forum adjourned at 10:51 a.m.)