AMENDED TRANSCRIPTION OF RECORDED STAKEHOLDERS SESSION

OF CALIFORNIA PRIVACY PROTECTION AGENCY

MAY 6, 2022

VIA TELECONFERENCE

Present: ASHKAN SOLTANI, Executive Director
BRIAN SOUBLET, Interim General Counsel
JENNIFER URBAN, Chairperson
TRINI HURTADO, Conference Services Coordinator

Transcribed by: DeEtte Hicks,
eScribers, LLC
Phoenix, Arizona

--o0o--

**AMENED TRANSCRIBED RECORDED PUBLIC MEETING**

**OF CALIFORNIA PRIVACY PROTECTION AGENCY**

**May 6, 2022**

**MR. SOUBLET:** (Audio begins mid-sentence) -- of the California Privacy Protection Agency's May 2022 Pre-Rulemaking Stakeholder Sessions. My name is Brian Soublet and I'm the acting general counsel for the agency. Please note that this event is being recorded.

We're delighted to have so many stakeholders who have signed up for these three-day sessions. This event -- the stakeholder sessions -- is the agency's third pre-rulemaking activity. While subcommittees of the Board provided input to the previous activities, the process has now been turned over to the staff, who have organized the stakeholder sessions to further inform the rulemaking process.

I have some logistical announcements; I'll go over the plan for this session. First, let me sketch out the format of these stakeholder sessions, so everyone has a sense of how things will proceed. As you can see from the program schedule, which you will find on the meetings and events page of our website, we are holding a series of stakeholder sessions this week. We started on Wednesday -- yesterday -- and today, May 6th.

During the sessions, we will be hearing from

stakeholders on a series of topics that are potentially relevant to the upcoming rulemaking. Those who signed up to speak in advance were, generally, given a speaking slot for their first choice topic. And we will be lim -- and will be limited to seven minutes. We will proceed through the program according to the schedule provided on the website. Please note that all the times are approximate and topics may start earlier or later than estimated.

You are welcome to come and go from the Zoom conference as you like, but if you have an assigned topic, we recommend that you make sure you are signed in before your topic session begins. Even if you did not sign up in advance, we still have an opportunity to speak during the time set-aside for general public comment at the end of the day today. Please take a moment to review the schedule to see when public comment is expected to occur. And again, please note that the times are approximate.

Each speaker making a general public comment will be limited to three minutes. We are strictly keeping time for all speakers in order to accommodate as many stakeholders as possible. Speakers that are scheduled for the current session on consumers' rights to limit use of sensitive personal information should be signed in to

the public Zoom meet using their name or their pseudonym and email they provided when they signed up to request their speaking slot. If you are participating by phone, you will have already provided the phone number that you're calling from, so that we may call you during your pre-appointed speaking slot. Note that your name and phone number may be visible. Sorry about that.

When it's your turn, our moderator will call your name and invite you to speak. If you hear your name, please raise your hand when your name is called, using the raise your hand function, which can be found in the reaction feature at the bottom of your Zoom screen. Our moderator will then invite you to unmute yourself and invite you to turn on your camera, if you wish. You will have seven minutes to provide your comments. In order to accommodate everyone, we will be strictly keeping time. Speaking for a shorter time is just fine. When your comment is completed, the moderator will mute you.

Please plan to focus your remarks on your main topic. However, if you'd like to say something about other topics of interest at the end of your remarks, you are welcome to do so. You are also welcome to raise your hand during the portion at the end of the day set-aside for general public comment. Finally, you may send us your comments via physical mail or email them to

regulations@cppa.ca.gov by 6 p.m. this afternoon.

California law requires that the CPPA refrain from using its prestige or influence to endorse or recommend any specific product or service. Consequently, during your presentation, we ask that you also refrain from recommending or endorsing any specific product or service.

I now ask the stakeholders who have been assigned the topic of consumer rights to limit the use of sensitive personal information be ready to present. Please -- again, please use the raise your hand function in Zoom when your name is called, so that our moderator can easily see you. As noted, the moderator will call you in alphabetical order by last name. We will now move to hear comments on this topic.

Ms. Hurtado, would you please call our first speaker.

**MS. HURTADO:** Yes. Good morning. Our first speaker is Andrew Crawford.

Okay. Mr. Crawford, you have seven minutes to speak. I see you're using your camera. Your time starts now.

**MR. CRAWFORD:** Thank you to the CC -- or CPPA for the opportunity to join you today. My name is Andrew Crawford. I'm a senior policy counsel at the Center for

Democracy and Technology. CDT is a nonprofit, nonpartisan, 501(c)(3) organization based in Washington, D.C., that advocates for civil rights and civil liberties in the digital world. For the past two years, I focused my work around identifying and advocating for robust privacy protections for consumers' sensitive data, focusing mainly on health data.

Appropriate collection, sharing, and use of sensitive data, like health data, can empower individuals in, you know, truly remarkable and beneficial outcomes. However, sometimes the benefits are more minimal and sensitive data collection, sharing, and use can be harmful. Specifically, when sensitive data is shared and used in ways the consumers do not want or anticipate, they lose agency over their data and face a greater likelihood of harm. Unfortunately, there are ample examples of consumers being harmed by inappropriate collection, and sharing, and use of sensitive personal information.

Reproductive help apps have been found to violate their own policies when sharing sensitive health information; millions of users with third parties, including advertisers. Moreover, just this week, there are news reports detailing how data brokers sell location information about visitors to health clinics, including

those that provide reproductive health services. The harms associated with the misuse of sensitive personal data can have lasting emotional and physical affects.

Today, the burden of protecting their sensitive health information and their sensitive data falls almost entirely on consumers. It's time to rebalance these relationships and empower consumers with more control over their sensitive information; how it's collected, how it's shared, and how it's used. To take full advantage of the current opportunity to confront these very real harms, the CPPA should embrace the following priorities in any subsequent rulemaking regarding sensitive personal information.

Number one, CPPA should embrace a broad definition of sensitive personal information. I encourage you to interpret CPRA's definition of sensible -- sensitive personal information broadly, so that it captures the full universe of this data pack. This is especially true when approaching health data. I encourage you to focus, not just on specific clinical data sets, data held by hospitals and doctors' offices, but more so on the nature of the data and how it's used. If data is being used by a business to make insights or conclusions about consumers' physical or mental health, that data should be treated as sensitive data. Indeed, any data can be

sensitive health data if it is used for those purposes, even if it appears unrelated on its face. Data sets like location information, web browsing history, and purchase histories can all reveal very probative details about consumers' health.

This type of purpose and use-based approach has several benefits. First, it benefits consumers by raising the bar for all data that's used to impact their health and wellness. Trying to delineate certain data sets as worthy of coverage and others as not no longer makes sense for people whose information is implicated. Second, this approach also creates a tech neutral standard that will stay relevant as technology evolves.

Next, CPPA should narrowly define what reasonable expectations by average consumer are when requesting goods and services. Under CPRA, it is up to each consumer to request that businesses limit the use of their sensitive information. Once that choice has been made, it should be meaningful and effective. To that end, you should embrace a narrower interpretation of what is reasonably expected by an average consumer who requests goods and services. As my colleague noted in earlier sessions that focused on data minimization and limitations, there are lots of examples of apps and services collecting far more information than is

necessary. If not constrained, there is a real risk that reasonable expectations can include unrelated -- can be -- can include data for unrelated purposes and uses that are not reasonably expected.

You should work to ensure that irrelevant data, especially sensitive information like health data, is not collected and retained when the data is unrelated to the goods or services being requested. Specifically, you should clearly articulate that, once a consumer directs a business to limit the use of his or her sensitive personal information, that business immediately acts. Immediate action includes businesses notifying third parties and service providers. This final point is important because consumers will often not know each and every third party.

Next, the consumer opt-out process should be simple and straightforward. For consumers to truly be empowered and gain back some semblance of control over their sensitive personal information, the choice to limit business use of their sensitive data should be simple to identify and easy to execute. You should develop rules that allow consumers to know their rights and exercise them easily.

First, timely and meaningful notice allows consumers to make informed decisions before they permit their

sensitive personal information to be collected, disclosed, or used. Sensitive information, like health data, is personal and intimate, and notices about it should not be relegated to a dense paragraph in a daunting, multi-page privacy policy. Instead, consumers should be prominently told about their rights to limit the use and disclosure of sensitive personal information independently of other terms and policies. Moreover, this notice and opportunity, beyond doubt, should be given before any collection or sharing has occurred.

But simply providing an initial notice is not enough. Consumers' rights to limit the use and disclosure of sensitive personal information data vanish once they've shared data with business -- with a business the right to continue and permit consumers to limit the use of collection at any time. CPPA should promulgate rules that provide ongoing transparency requirements at set intervals to allow each consumer to revisit their decision. Periodic notification should be simple and digestible in order to best empower consumers to revisit their decisions and to make new ones regarding how businesses use some of their most sensitive personal information.

These notices should also be provided in ways that are accessible to all consumers. And rules you develop

should ensure that notices are tailored for each set of users and made easily to access and understand. Consumers aren't empowered if they don't know about and have the ability to review --

**MS. HURTADO:** Thirty seconds.

**MR. CRAWFORD:** -- their rights to limit the collection and use of sensitive personal information.

So to wrap up, I commend CC -- CPPA for holding these sessions. I'm happy to serve as a resource moving forward and I thank you, again, for your time.

**MS. HURTADO:** Thank you so much for your comment. Our next commenter is Leticia Garcia. Thank you.

Okay. Ms. Garcia, you have seven minutes to speak. You may use your camera, if you wish. Your time starts now. You're muted, Ms. Garcia.

**MS. GARCIA:** Hi. Good morning. My name is Leticia Garcia and I'm the director of state government relations for the California Grocers Association. CGA is a nonprofit, statewide trade organization representing the food industry since 1898. CGA represents approximately, like, 500 retail members operating over 6,000 food stores in California and Nevada, and approximately 300 grocery supplier companies. Traditional supermarkets in California employ over 300,000 residents in virtually every community in the state.

Thank you for the opportunity to be here and give our perspective. The grocery industry has many aspects to it and we deal with a vari -- wide range -- wide range of issues in order to be able to provide essential services throughout the state. We are not here to get into technical concerns with the proposed regulations, as it's not the grocery industry -- grocery industry's main focus. We defer to our business partners, whose main advocacy is on privacy issues.

I am here today to express how this proposed regulations can potentially destruct our members' day-to-day operations. The primary topic I would like to touch on is the consumers' right to limit use of sensitive personal information. If time permits, I will also like (audio interference) automated decision making.

We have two main concerns in regards to this section. One being how this would affect individuals who participate in the WIC and SNAP programs. And the second being on how this would impact our human resources and hiring departments. Rules regarding the use of sensitive personal data should not apply in circumstances where the data has been de-identified or such user disclosure is reasonably necessary to provide the services the consumer has requested.

In California, 49 percent of households with

children participate in the SNAP program; and for WIC, 82 percent of Californians eligible for WIC have received benefits. SNAP is an essential program to ensure families and individuals who find themselves to be food insecure receive the essential benefits of purchasing food. WIC's main focus is to ensure children receive food that will help their development in their first years of life. The unprecedent nick -- the unprecedented nature of COVID shifted much of our business model and for the first time, we saw a great push for customers to pur -- to purchase groceries online and have them delivered or be ready for curbside pickup. Because of the increase in online shopping and the unknown dangers of COVID, the USDA Food and Nutrition Services -- FNS -- decided to allow SNAP participants to also purchase groceries online. This is a pilot program whose timeline was expedited and made available in almost all SNAP participating stores. WIC is currently in the process of considering online shopping and we anticipate the transition is coming in future years.

FNS is very strict on guideli -- on the guidelines of the programs, and any deviation from these guidelines can result in participating stores to either have their partition -- participation suspended or revoked. Federal requirements on data collection and storage of these

programs need to be taken into consideration, given the use of it to evaluate these programs. We ask you to truly consider the impact of these proposed regulations will have on our WIC and SNAP retailers.

The second and last point I would like to touch on is on the HR pro -- process. The processing of personal information in the HR context should be excluded from such regulations. Regulations would result, primarily, in significant costs and confusion, conflicts with federal and state employment laws governing personal information in the HR space, and impair the ability to exercise and defend against legal claims. Sensitive personal information collected in the HR context is, primarily, not collected to infer character -- characteristics about a consumer, but rather for a variety -- a legitimate purpose in order to comply with state and federal laws.

We not only represent large chain stores that can afford to hire an expert in privacy law to comply with these regulations, we also represent small, single -- single store and independent operators. Our industry runs on very small profit margins ranging from two to four percent. Our smaller retailers will find it difficult to try to comply with such a complex law on their own, as they are not experts in privacy law. These

smaller retailers only want to feed their community and not have to go through the reg -- regulations with their HR personnel. Any risk of the privacy individuals -- any risk of the privacy of individuals in the HR context is far outweighed by the burden such regulations would place upon businesses in the HR space.

That's it for my first topic. I would like to now switch over to the topic of automated decision-making technology.

Automated decision-making technology and profiling should be limited to activities that require the processing of personal information. Automated technology has significant benefits to both businesses and consumers, including enhanced accuracy and consistency, safer and more innovative products, scalability, cost savings -- cost savings and increased efficiencies. Accordingly, we ask the Board to be mindful about providing consumers any right to opt out of automated activities, as it could severely hamper businesses and other consumers' ability to realize those advantages.

Specifically, in the grocery business, our members are not in the business of tracking such information. The automatic decision-making technology that is used provides better access of groceries to their customers. Adding this additional tracking information will take

away resources for other necessary services that grocers provi -- provide, such as philanthropic endeavors, locating additional store locations, and other -- and other services. We also use these automated decision-making technologies to enhance our customer service experience through their loyalty programs and weekly ad alerts. These programs help our customers receive the coupons and discounts on items they frequently purchase.

Again, we're not in the business of storing and tracking data.

**MS. HURTADO:** Thirty seconds.

**MS. GARCIA:** Our primar -- primary business is to feed the communities we serve. We ask that you consider the impacts of these regulations on the grocery industry, especially on our smaller, independent store operators. Thank you.

**MS. HURTADO:** Thank you so much for your comment. Our next speaker is Alan Sege, S-E-G-E.

Okay. You have seven minutes to speak. Your time starts now.

**MR. SEGE:** Thank you, Ms. Hurtado. Thank you, Mr. Soublet and the agency staff. And thank you, all the stakeholders, who are attending. I -- I thank you for giving us this opportunity to present this morning. My name is Alan Sege, and I and -- and my firm represent

technology and media companies here in California. And we assist our clients in protecting consumers' privacy rights but primarily, I present to you today as a citizen of California.

I'm here to talk with you about a practice amongst some sellers of business databases, which are very disturbing in the extent to which they appear to violate the CPRA's very important new protection over the collection and the consumers' right to control their own sensitive personal information. I've also presented the facts in the law about this practice in my written submission. These are practices that seem to violate also the base requirement under the old law and under the new law, entitling people to be informed "at or before the point of collection", of the categories of personal information that are being taken from them and the purposes for which they're being used.

And here's what the practice is. Imagine yourself emailing somebody at their work email address. It could be your boyfriend or your girlfriend, it could be your spouse. You could be a psychologist emailing your patient who works at a company. You could be an attorney for the com -- for the company, itself, emailing your client. You could be law enforcement emailing a witness or a victim. But there's something that the person

you're emailing doesn't know and this is something that you, the person sending the email including sensitive contents, you can't -- you can't possibly know. And very often, or even usually, even the company who employs the recipient and who runs the email server doesn't know.

You have become a data subject because the company that runs that email happens to subscribe to a major business database service, like Dun & Bradstreet or ZoomInfo. And somewhere deep in some fine print -- it could be in a click-through agreement executed by the IT guy at the company -- that ZoomInfo customer gave ZoomInfo access to all of the company's inbound emails. And ZoomInfo says that they just scrape the emails, using what they call advanced artificial intelligence techniques, only for what they call "email signature information". They say that's like your email address, your office phone number, it could be your direct dial phone number, your title, the person you report to, it could be your cell phone number. And that they receive the entire contents of the email, but with their artificial intelligence, they scrape it for what they determine to be just business contact information. These companies, like ZoomInfo and Dun & Bradstreet, perhaps others who engage in this practice, add to their commercial database all that information that they scrape

to the tune of hundreds of millions of dollars per year. And the practice is growing in prevalence.

Of course, because those purva -- those database purveyors could not have known that you were planning to send an email, you were never informed "at or before the point of collection" as required under the -- under the CCPA and under the CPRA Section 1798. By the way, their tech often doesn't work. As we -- as we exhibit in our written submission, without even really trying, we found examples of ZoomInfo publishing the contents of emails, even including attorney-client privileged contents of one of my colleagues who co-authored our submission. This practice, which our submission tactfully terms direct data extraction, seems to me to be a complete violation of the requirements under existing law, and even more so under the new law.

Under the new CPRA, the contents of an email are named explicitly as sensitive personal information, entitling the consumer to full information before collection and near complete control over its harvesting and use. This practice, though, has become extremely widespread, even since the enactment of the CPPA -- of the CCPA. The databases, including the personally identifiable information that I referred to, now subsume what I believe to be a large majority of adult

Californians. And you can verify this; you can check yourself. Just Google the name of almost anybody you know, plus the word -- one word -- ZoomInfo. This takes you to a public version of ZoomInfo, which they use to promote their paid service. They show you some of the fields of information they've scraped from emails and published about the person. By their own public statements from more than one year ago, ZoomInfo, alone, collects sensitive personal information extracted from consumers' inbound emails and CRM systems over fifty million times every day.

Enactment of the CCPA had no effect on deterring this practice of direct data extraction, which has only grown more prevalent over the past few years, as the office of the Attorney General of California took no action. But I have to note at the same time, a number of reliable commercial business data providers --

**MS. HURTADO:** Thirty seconds.

**MR. SEGE:** -- competitors of ZoomInfo and Dun & Bradstreet -- refuse to engage in this direct data extraction method under the belief that the CPRA prohibits it or they don't wish to test the limits of the law. Coincidentally, ZoomInfo seems to agree that clarification or rulemaking is needed, but they ask in their submission, essentially, to be the arbiter and to

let their technology determine what parts of an email they can extract and (audio interference) and which they can --

**MS. HURTADO:** Mr. Sege.

**MR. SEGE:** Yes.

**MS. HURTADO:** Time.

**MR. SEGE:** Okay. Well, I -- I thank you for your time. And I and my friends are happy to remain a resource to you and to make our materials and research available to you for your deliberations.

**MS. HURTADO:** Thank you for your comment. Our next commenter is Hayley Tsukayama.

Hayley Tsukayama?

Okay. Brian, that was our last commenter.

**MR. SOUBLET:** I'd like to thank everyone for participating in this morning's session. We're going to take a short break and come back at 10 a.m. for -- the session will be on the processing that poses a significant risk to consumers. Feel free to leave the video or teleconference open, or to log out and back in at 10 a.m. when that next session starts. Thank you.

(Whereupon, a recess was held)

**MR. SOUBLET:** It's 10 a.m. Good morning and welcome back to the California Privacy Protection Agency's May 6th Pre-Rulemaking Stakeholder Sessions. The topic this

session is processing that poses a significant risk to consumers. Speakers that are scheduled for this session should be signed in to the public Zoom link, using the name of pseudonym in the email they provided when they signed up to request their speaking slot. Speakers will be called in alphabetical order by that last name during this window, and will not be able to -- and you will not be able to speak if we miss your slot.

When it is your turn, our moderator will call your name and invite you to speak. If you hear your name, please raise your hand when your name is called, using the raise your hand function, which can be found in the reaction feature at the bottom of your Zoom page. Our moderator will then invite you to unmute yourself and also invite you to turn on your camera, if you wish. You will have seven minutes to provide your comments.

In order to accommodate everyone, we will be strictly keeping time. And speaking shorter than your length of time is just fine. When your comment is completed, the moderator will mute you. Please plan to focus your remarks on your main topic. However, if you'd like to say something about other topics of interest at the end of your remarks, you are welcome to do so. You are also welcome to raise your hand during the portion at the end of the day set-aside for general public comment.

You may also send us your comments via physical mail or email them to regulations@cppa.ca.gov by 6 p.m. today.

California law requires that the CPPA refrain from using its prestige or influence to endorse or recommend any specific product or service. Consequently, during your presentation, we ask that you also refrain from recommending or endorsing any specific product or service.

One presenter in the last session had not confirmed their speaker spot. In fairness to all of our presenters today, we had to move on. But we would invite that speaker to join our public comment session at the end of the day, raise your hand, and we will allow you your three minutes to speak.

I now ask that stakeholders who have been assigned to this topic, which again is processing that poses a significant risk to consumers, to be ready to present. Please use your raise your hand function in the Zoom when your name is called, so that our moderator can easily see you. As noted, the moderator will call you in alphabetical order by last name. We will now hear those comments.

Ms. Hurtado, please call our first speaker.

**MS. HURTADO:** Okay. First speaker for this session is Max Behlke.

Okay. Mr. Behlke, you have seven minutes to speak. Your time begins now.

**MR. BEHLKE:** Thank you. And I don't think I'll need all seven minutes. My name is Max Behlke. I'm the director of state government affairs for the Electronic Transactions Association. ETA is the trade association that represents the broad group of companies that provide electronic products and services, including mobile wallets, computer products, credit and debit cards, and other forms of dibit -- digital payments. Ours is an industry that, in North America, moves over 8.5 trillion dollars a year in card and P2P payments securely, reliably, and quickly. In fact, during the time allotted to me today, nearly two million transactions will be processed.

As the California Protection Agency continues its preliminary information gathering and contemplates updating and crafting regulations, I appreciate the opportunity to provide these brief remarks. We believe they deserve consideration as you craft rules to achieve the law's objectives.

First, regarding the processing of personal information in the payments industry. ETA and its members strongly support a privacy framework that allows companies to implement innovative tools to protect

consumer privacy and data, while fighting fraud. An industry where data security and -- and consumer protection are foundational -- foundational pillars in protecting the payment's ecosystem. The payments industry makes dedicated efforts to use innovation to fight fraud and ensure the consumers have access to safe, convenient, and affordable payment services.

Processing of personal information in any environment for fraud prevention and anti-mono -- anti-money laundering processes, screening or compliance with legal obligations should be exempted from the scope of this definition or regulation. These activities protect consumer's privacy and security. And -- and industry keeps such activities confidential to prevent bad actors from gaining insight into our internal systems.

There should be appropriate carveouts for any processing related to fraud prevention, anti-money laundering services, screening, or -- or any anti-theft security or compliance services. Companies often must work with the third party providers to support these activities, so providing the consumer the opportunity to opt out would substantially hinder a company's ability to protect consumers.

I'd also just like to briefly comment on cybersecurity audits. It's important to note that

businesses in the financial industry already perform industry standard audits and reports. For example, storage of payment cards on file is regulated in the industry by the PCI-DSS standards and merchants are regularly required to certify each year. And these circumstances, the payments industry should be able to reuse such audits certifications, rather than duplicate their efforts, which would be -- unduly add to the cost and burden of compliance.

As I said, I was going to keep my brom -- comments brief and I appreciate you taking the time to consider our remarks today.

**MS. HURTADO:** Thank you so much for your comment. Our next commenter is Neil Chilson.

Neil Chilson, please raise your hand.

Okay. We'll move on to Johnny Ryan. Johnny Ryan, please raise your hand.

Mr. Soublet.

**MR. SOUBLET:** Thank you. We'd like to thank for that comment that we just had. Unfortunately, our other two confirmed speakers for this session are not here now. So we're going to, again, take a break and be back at 11 o'clock for our session on cybersecurity audits and risk assessments.

Actually, what I think I'm going to do. I'm going

to wait a couple of minutes. We'll stay on screen and see if either Mr. Chilson or Mr. Ryan appear, since we have some time.

So I'll call out first Neil Chilson. If you're there, please raise your hand.

Okay. Mr. Johnny Ryan, if you're logged on, please raise your hand and we can hear your comments.

Okay. Just as a reminder, when we start our sessions, if you're here, we're going to be calling your name alphabetically. So if you've signed up and reserved a speaking slot, please make sure to log in right at the allotted hour when we're moving to your session.

So now we're going to go ahead and take that break and be back again at 11 o'clock for cybersecurity audits and risk assessments.

Oh, there's Johnny Ryan.

**MS. HURTADO:** Mr. Ryan, can you please raise your hand?

**MR. RYAN:** Hi.

**MR. SOUBLET:** Thank you.

**MR. RYAN:** Sorry about the delay there. Oops. (Indiscernible) the camera. There we go. Okay. That should work better. Hopefully, you can hear me okay.

**MS. HURTADO:** Yes. Please continue. You have seven minutes. Your time starts now.

**MR. RYAN:** Okay. And thank you for having me and letting me represent my views here. I'm going to share my screen to show you a few slides. What I want to do is take you through what happens when you visit the average website or app and you, as an internet user, what happens to your data.

And when you go to a conventional website, the website is trying to figure out what ads should be shown to you. So information about you is sent out to at least one ad exchange or ad auction. And that ad auction has -- sends the information out to one or more, and possibly a large number of parties who can bid on the opportunity to show you their ad. These are called DSPs. In theory, the right DSP gets the opportunity to show you their ad. But the problem is, we actually don't know what happens to the consumer's data in that situation.

Now, let me give you an example of -- of -- of one DSP that we know about. This is a company called Vectuary. Very, very small. Three and a half million Euro turnover, so we're right about four million dollars. And it was investigated by the French enforcer in 2018. Now, the French enforcer found that just by sitting in on these auctions that I've described, this company had hoovered up 67.7 million people's data. Now, when you visit the website, it makes this claim that it protects

your privacy, and actually, it makes another claim. It says we might collect a lot of data, but we only store 30 percent of it and we dump everything after a year. Which begs the question, did this tiny company -- just one among many -- actually hoover up a huge quantity of different people's data in a very short amount of time?

So let me take you through the process of what happens when you visit a website, and I'll slow it down. This normally happens in a split second as you're loading the page. These -- the SSP, an ad tech company working for the publisher, sends information about you to at least one of these ad exchanges, and the ad exchange sends information about you to many of these DSPs and one of them wins the auction. It makes the winning bid and its ad is shown to you. Now, the impression you should have when you look at this diagram is, that is an awful lot of arrows. What I want to make you think about, though, is what information about the consumer and what risk to the consumer is created by those arrows.

So we know what is going out about the consumer. We know this because there are two industry specifications, which are public documents. Here they are and they tell us what can be sent out in these broadcasts. Now, I'm going to show you, from one of the documents, an example of one of these broadcasts and take you through what

happens. What you're seeing here is unique identifiers about the person, the person's age, more information about their device, and where this young lady, in this case, is standing. Now, that's quite sensitive data. But in addition, there's also information about the kind of material that she is watching. Now, we know this is a -- a depreciated industry document, but it seems to be out there in the wild. We know that, from industry documents, thousands of companies can be receiving these data every time an ad is shown, potentially, and there's no way to control what happens to the data. That sounds like a data breach. Certainly, it sounds like sharing and cross-context behavioral advertising run amok, I would suggest.

The next question is, what's the scale? Well, let's take a look at a single one of those ad exchanges that I described. And here is a list from Microsoft's ad exchange. They just bought it; it's called Xandr. This is the list of companies that Xandr says it can share your data with when you visit a website. And we're scrolling -- I'll save you the full list -- through 156 -- say four pages -- of 1,647 companies. And Xandr is only one of these auctions. So what we're talking about here is the biggest data breach ever recorded. And it's not enough to know that these data by consumers are

being shared wildly in this way, but it also allows us an insight into the information that goes into profiles about us and how we then might be manipulated.

Now, we can know what those profiles now look like, because of documents like this. This is the IAB Tech Lab Audience Taxonomy, version 1. And I'll show you the kind of categories that the tracking industry is using to put into profiles about all of us. For example, here are the codes that define your religion -- Buddhist, Christian, Hindu, et cetera. Your mental health, whether you're infertile, have STDs, if you're interested in weight reduction. And the taxonomy even looks at the most sensitive parts of the person. Life -- the person's life, whether you have a -- a special needs child, for example. And if that's the case, the industry code is 357. And of course, this extends to what are your political views?

Now, it is clear that this kind of information about a person should not be shared in this way in the wild. And it certainly should not be shared with foreign companies and it shouldn't be as sensitive as it currently appears. So what I'm describing is an underlying data free-for-all in the online advertising industry.

And what I want to finally wrap up and suggest is

that even that industry understands the need for a solution. So IAB Europe has just published in the last few months this document, in which is argues that the contextual advertising industry will be a 412 billion dollar industry by 2025, and they have various statistics saying this is a good thing.

And finally, let me leave you with one chart. This is four years of -- of advertising revenue from a European publishing group that did switch its advertising. And I want to go to the bones.

**MS. HURTADO:** Thirty seconds.

**MR. RYAN:** The GDPR and COVID-19, and you will see that when they made the switch, the revenue went up. And I'll leave you on that point. Thank you.

**MS. HURTADO:** Thank you so much for your comment.

**MR. SOUBLET:** We're going to try one more time to see if Mr. Neil Chilson is on. And if you are there, please raise your hand so that we may allow you in for your comments. Again, that's Neil Chilson.

Okay. Well, we're going to take our break now and we'll be back again at 11 o'clock with cybersecurity audits and risk assessments. So if you have signed up for that topic, please be ready to go at 11. Thank you.

(Whereupon, a recess was held)

**MR. SOUBLET:** Good morning. It is 11 a.m. And for

those of you that were with us earlier, welcome back. This is the California Privacy Protection Agency's May 6th Pre-Rulemaking Stakeholder Session. As a reminder, our sessions are being recorded. Speakers that are scheduled for the current session on cybersecurity audits and risk assessments should be signed in to the public Zoom link, using their name or pseudonym and the email they provided when they signed up to request their speaking slot.

When it is your turn, our moderator will call your name and invite you to speak. If you hear your name, please raise your hand when your name is called, using the raise your hand function, which can be found in the reaction feature at the bottom of your Zoom screen. We will then invite you to unmute yourself and invite you to turn on your camera, if you wish. You will have seven minutes to provide your comments. In order to accommodate everyone, we are strictly keeping time. However, if you speak shorter, that's just fine.

When your comment is completed, the moderator will mute you. Please plan to focus your remarks on your main topic. However, if you'd like to say something about topics of interest at the end of your remarks, you are welcome to do so. You are also welcome to raise your hand during the portion at the end of the day set-aside

for general public comment. You may also send us your comments via physical mail or email them to regulations@cppa.ca.gov by 6 p.m. this evening.

California law requires that the CPPA refrain from using its prestige or influence to endorse or recommend any specific product or service. Consequently, during your presentation, we ask that you also refrain from recommending or endorsing any specific product or service.

I now ask the stakeholders that have been assigned to the topic of cybersecurity audits and risk assessments be ready to present. Please use the raise your hand function in Zoom when your name is called so that our moderator can easily see you. As noted, the moderator will call you in alphabetical order by last name. We will now hear those comments.

Ms. Hurtado, please call the first speaker.

**MS. HURTADO:** Yes. The first speaker for this session is John Davisson. Thank you.

Okay. Mr. Davisson, you have seven minutes to speak. Your time begins now.

**MR. DAVISSON:** Good morning. And thank you for the opportunity to present today. I'm John Davisson, director of litigation and senior counsel of the Electronic Privacy Information Center, or EPIC. EPIC is

a nonprofit public interest research center established in 1994 to protect privacy, freedom of expression, and democratic values in the information age. As relevant to today's session, EPIC has a long history of advocacy, public education, and litigation concerning the role of risk assessments, privacy impact assessments, and algorithmic impact assessments in the protection of personal data.

Although we are mindful of the limitations of risk assessments, we believe that, when used as part of a comprehensive data protection regime, risk assessments can be a powerful mechanism for minimizing the collection, use and misuse of personal data, for ensuring that institutions are forced to weigh the privacy risks of their planned activities, and to justify those risks legally and normatively. And for keeping institutions accountable to the public with respect to the collection and use of their personal data.

Gary Marks has written that the object of a risk assessment is to anticipate problems, seeking to prevent, rather than to put out fires. We urge the agency to implement the risk assessment provisions of the CPRA with this purpose in mind. EPIC provided recommendations concerning risk assessments in our comments to the CPPA in November, and we anticipate providing further written

recommendations on this subject in the future. But I'd like to highlight four points today.

First, although the categories of risk assessment information set out in the CPRA are essential, the agency should strengthen and broaden these requirements through its regulations. Without going into the detail about every category of information assessments should include, we would refer the agency to the privacy impact assessment provisions of the E-Government Act of 2002, the OMB guidance implementing the E-Government Act, and Article 35 of the GDPR for examples of the types of information and analysis that risk assessment should include.

Second, in assessing risks to the rights of consumers, businesses should be required to evaluate the full range of privacy harms and civil rights violations that may result from the processing and disclosure of personal data. Too often risk assessments focus on the narrow question of whether personal data collected by an institution is secure from breaches. Although this is an essential element of data protection and one that is built into the CPRA's requirement for annual cybersecurity audits, it is only the beginning of a more robust analysis that institutions must undertake when processing personal data. Businesses must consider, not

only the unintended and -- the harms, rather, from unintended or unauthorized uses of data, but also the harms from intended uses of data, including screening, scoring, and other forms of algorithmic decision making. Businesses must also account for the full range of harms that can result from the processing and misuse of personal information.

Profs. Danielle Keats Citron and Daniel Solove have recently mapped out this spectrum, which includes numerous physical, economic, reputational, psychological, autonomy, discrimination, and relationship harms. And businesses must take special account of the uneven impact that data processing and potential misuse can cause, which disproportionately harms people of color, low-income individuals, and other marginalized populations.

Third, ensuring the right timing and frequency of risk assessments is critical. As reflected in the CPRA's requirement of regular risk assessments, an assessment cannot be treated as a static one-off undertaking. Rather it is a process, which should begin at the earliest possible stage when there is still an opportunity to influence the outcome of a project or activity, and should continue until or even after the project or activity has begun. We urge the agency to require the completion of a risk assessment as soon as a

business takes material steps for its data processing that will present significant risk to the consumers' privacy or security. This will ensure that the risks to individuals can be prevented or mitigated before any processing begins. Allowing risk assessments to be popo -- postponed until the last minute, or even after data processing has begun, would allow risk assessments to become a box checking exercise and facilitate the whitewashing of harmful data practices.

We also urge the agency to require covered businesses to review, update, and resubmit privacy risk assessments well in advance of a change to a business's data processing activities that might alter the resulting risks to privacy. In any event, businesses should be required to conduct such a review no less than once per six-month period.

Finally, it is important for the CPRA and the business submitting a risk assessment publish the results of the assessment promptly, conspicuously, and by means that are readily accessible to interested members of the public. In addition to forcing businesses to evaluate and mitigate the harms of data processing, a risk assessment also serves to inform the public of a data collection or a system that poses a threat to their privacy. Although the CPRA already requires the agency

to provide a public report summarizing the risk of assessments -- the risk assessments filed with the agency, we believe the underlying assessment should be presumptively public, subject only to the narrow redactions necessary to protect data security and trade secrets. This added degree of transparency will significantly enhance the data protection benefits of the CPRA, without imposing significant additional burdens on businesses that are already required to produce the risk assessments.

That concludes my remarks. Thank you, again, for the opportunity to speak today. And we look forward to helping the CPPA develop and implement robust risk assessment regulations.

**MS. HURTADO:** Thank you so much for your comment. Our next commenter is Odia Kagan.

Okay. Ms. Kagan, you have seven minutes to speak. Your time begins now.

**MS. KAGAN:** Thank you. Hello, everybody. And thank you very much for the opportunity to present here. My name is Odia Kagan. I am a partner and chair of a GDPR compliance and international privacy at Fox Rothschild. And as such, I work a lot with companies -- U.S.-based and multi-nationals -- on both U.S. and GDPR compliance. And as you know -- and that's how I've been dealing with

clients with DPIAs, and speaking with my privacy friends and colleagues in Europe about their experiences.

So I -- I polled my colleagues and clients and would like to spend some of my seven minutes on some do's and don'ts, based on the EU experience. And this really ties into what John was saying just now about the specificity of the regulations. So I want to make three main points.

The first one is, I think the regulations definitely need to be more robust and give the guidelines. But there's no real need to reinvent the wheel. There is a little bit of specificity in the Virginia and in the Colorado laws, but there is really a lot of work that has been done in Europe that can be leveraged. This is going to be -- you know, using the EU experience -- not necessarily applying it, you know, verbatim as the model -- but using it has a lot advantages. One, because it is faster to get off the ground, seeing as the compliance date, you know, is -- is coming up for companies. But also for both purposes of legal certainty, and also ease of compliance for companies. Because there are a lot of multi-nationals that already have DPIAs that have been done in Europe. And if the -- the principles and the requirements are close enough, they will be able to leverage them, make the necessary adaptations, and use them in the U.S. (indiscernible).

So that's the first one.

The second point is, I think that really there needs to be clear guidance, but not too specific guidelines for when a DPIA is needed or a risk assessment on the data protection is needed. So you know, Brene Brown says clear is kind and unclear is unkind. When you have a general principles, it's very difficult to implement them. Also, you run against issues where companies doing -- are doing what they think they need to do, but it's not actually what it was supposed to be. So parameters for when a DPIA is required would be a really good idea.

The European model of proposing, you know, general principles -- here are nine situations where if, you know, two of them happen, is a good idea. That one big pet peeve of European practitioners and companies are if not having some sort of decision tree. Like, some sort of decision tree of looking at the solutions would be helpful. But it's also important not to be too specific.

There's actually -- the European data protection board has actually sent back for revision DPI blacklists from member states that were too specific, and for example, flag -- flagged just processing sensitive data, or just cross-border transfers, as requiring a DPIA. Another option is having some sort of, like, a, you know,

sort of a less detailed DPIA for certain situations.

The other is -- another issue is the views of harm and theoretical views of harm not being too vague. The other option or recommendation is to consider predic -- pro -- providing whitelists, which -- here are things where, if this happens, you probably don't need a DPIA at all. Another point that we heard a lot is trying to define the role of the service providers, both in assisting the company to do its own DPIA, and the big providers, like, you know, big tech companies that are service providers, in leading the charge and helping the market and the industry having DPIAs available to inform their processes, as we've seen in Europe and the Netherlands recently with a couple of providers.

And the other is, as John was mentioning, this is not a standalone. It's part of your company's processes, and it's really important to get -- to get guidance on how it incorporates into the company's processes. And then the third point is, provide clear but not too complicated guidelines for how to carry out the DPIA. Here also, it -- it's a good idea to leverage what we have from the EU but make the re -- the relevant adaptations. We have models from the UK, from France, from Spain. There is an ISO standard, 29134. Maybe that -- maybe, you know, leverage that in an updated way.

And -- and of course, the interplay between an information security management system and the privacy risk assessment on top.

In Europe, the ICO model, for example, is very simple and easy to understand -- user friendly in understanding. But there are those in Europe that are saying that it doesn't delve into the specificity of analyzing the harms. John was mentioning, we have our own -- we have, you know, the SOLUP (ph.) model, and CALO (ph.), and we -- that we can, you know, rely on. And then on the other end of the spectrum, there's the German model with very specific risk mitigation for each risk.

And maybe there is a -- sort of somewhere -- line in the middle that allows both companies that are small, and medium enterprises engage in this, because it's very important to find something which is not cost prohibitive and just not completely deterrent to smaller companies.

The other things that would be really helpful to have in this are determining the probability of occurrence, and also guidance on how to actually carry out the process. How to -- there is a 3D model that looks at processing phases, like storage, use modification, and processing stakeholders. Like, software, harder -- hardware employees or recipients. And for each of those --

**MS. HURTADO:** Thirty seconds.

**MS. KAGAN:** -- calculating the likelihood and the severity of the infringement.

I think the document -- the guidance should also be not only on how the document should be, but also how the process should be carried out in the companies. And also, the last point is, it would be helpful to have some sort of resources, repository of sample DPIAs, especially like Camille did in France, especially for things like high-risk algorithms or some model that companies could look and see what they can do. Thank you.

**MS. HURTADO:** Time, Ms. Kagan.

**MS. KAGAN:** Thank you.

**MS. HURTADO:** Thank you for your comment.

Our next commenter is Barbara Lawler. Thank you. Okay, Ms. Lawler, you have seven minutes to speak. Your time begins now.

**MS. LAWLER:** Good morning, thank you. Thank you to the CCPA for holding these stakeholder sessions, providing the opportunity for stakeholders to give feedback about the rulemaking. I'm Barbara Lawler. I'm the chief operations officer and senior strategist for the Information Accountability Foundation. The IAF is a nonprofit research and educational information policy think tank. Our mission is to foster effective

organizational accountability that facilitates a trusted digital ecosystem, and the ability for organizations to use data responsibility to create real value for people

We believe that to be trusted, organizations must be accountable, responsible, and answerable, and be prepared to demonstrate their accountability. We believe that frameworks based on risk assessments and effective data governance enable beneficial data-driven innovation, while protecting individuals in society from the potential harms that may arise from data processing in the digital age.

As the interests of multiple stakeholders increase, and expectations that organizations be accountable for the processing of data about people, risk assessments are a critical and necessary lynchpin of operational integrity for evaluating the risk to consumers' privacy and security. Since 2014, the IAF has led multistakeholder research projects that describe ethics-based assessment frameworks for complex and potentially risky processing.

Deciding the process data is, in itself, a risk-based action. This work includes global forms, as well as specific projects in the US, Bermuda, Canada, Singapore, Hong Kong, China, and Europe. Risk assessment frameworks function as a governance model for

organizations of all sizes and should be encouraged regardless of the type of data processing activity, or in anticipation of significant risks, as described in California Section CPRA on that topic.

Accountability-based risk assessments are responsive to both aspects of accountability, being both responsible and answerable. The objective for the risk assessment is to demonstrate, i.e., be answerable, that data processing is responsible, and that impacts to stakeholders are considered. Fundamentally, the question of who is impacted, people, and how, and whether others, as in other people, larger groups, or the public, are part of a risk-assessment that is demonstrable.

The risk assessment process creates the risk documents that provide a sustainable mechanism for the organization to be answerable, and to demonstrate that it is acting responsibly. To determine the risk of what, and to whom, a measure -- measurable vetted framework is needed to describe the impacts to people. That is, a framework of negatives to isolate and manage and measure against. The IAF created such a framework as part of our model legislation, the Fair and Open Use Act, which we've called adverse processing impacts. And it's derived from the already vetted NIST Privacy Framework.

Incorporating adverse processing impacts into risk

assessment serve broader purposes as well. It creates mechanisms for privacy by design and default. It points to controls that should be implemented and validated within the organization. It can inform usable and fair designs for consumers, and it creates a strong linkage with security risk assessments based on NIST or similar frameworks such as SOC and ISO.

It provides measurability for the organization, and equally important, as a means to measure and enhance the capability to oversee and review risk assessments by the agency. Although technical compliance is important, if that is the only focus, organizations will miss the bigger picture and strategic issues and considerations related to the processing of data about people. Therefore, accountability-based risk assessments should become the norm for structuring and implementing risk assessments, and the broader privacy and security governance for organizations as overseen by the agency.

Thank you. Detailed resources can be found on our website and will be included in links in our written comments that we'll also be submitting. We look forward to future discussion with the agency on this and related topics. Thank you.

**MS. HURTADO:** Thank you so much for your comment.

Our next speaker, commenter, will be Jake Parker

(ph.).

Jake Parker, if you're available, please raise your hand.

Okay, we'll move onto the next commenter, David Sullivan. Thank you. Okay, Mr. Sullivan, you have seven minutes to speak. Your time begins now.

**MR. SULLIVAN:** Good afternoon, thank you. My name is David Sullivan. I'm the executive director of the Digital Trust and Safety Partnership, a growing collaboration between providers of diverse digital services, to ensure a safer and more trustworthy internet. Our thirteen members, whose services range from search and social media to cloud and ecommerce, have aligned around a set of commitments, best practices, and assessments for what we call digital trust and safety. So we're aiming to document and facilitate the adoption of widely deployed, overarching commitments to foster greater transparency and better understanding of trust and safety inside and outside the tech industry.

So the overarching commitment for our members is really to account for what we call content and conduct-related risks across five domains, including product development, governance, enforcement, improvement, and transparency. And we think that these steps are something companies can take to address cer -- issues

around harmful content and conduct online, while hold -- upholding human rights' standards, and also upholding the social and economic value of digital services.

So we have published our best practices framework, which has an inventory of about thirty-five examples of practices across these commitments. And all of our partners embrace those commitments with each selecting a combination of practices that best mitigates the -- the particular content risks that their platform or service faces.

So we've also published a risk-based proportionate approach to assessing these practices, which we call the safe framework. And where the level of an assessment that a company needs to undergo is determined by looking both at the size and scale of the company, as well as the risks presented by its particular product or service. We're also going to be releasing an inaugural state of the industry report in the near future to provide industry level insights into the maturity of trust and safety practices.

This work is inspired by and really draws upon the formalizations and maturation of the cybersecurity discipline within the tech space, through efforts that other speakers have already cont -- noted, such as the NIST framework, ISO standards, and other audit and

assurance practices that provide objective and measurable means of assessing and mitigating cybersecurity or privacy risks.

Today, I think there's a high degree of interest, in California, across the United States, and around the world, around how companies are addressing what we call content and conduct-related risks, the illegal or harmful content found on digital services. So our aim is really to provide a common industry-based approach based on practices and standards that are content agnostic and are capable of responding to the content risks of today, and the ones tomorrow around the horizon we don't know about yet, backed by a robust accountability mechanism of third-party assessments.

So we're going to be looking to learn from the privacy and security risk assessments and audits required by the CPRA, as we develop our process, and likewise, amid proposals that the CPPA widen its scope to include nonprivacy matters, such as children's wellbeing, I would encourage you to look to our best practices and our assessment framework to understand the significant efforts that our members are undertaking when it comes to elevating and formalizing trust and safety as a discipline, and the value of sort of consensus industry standards, and this approach.

So with that, I really look forward to further opportunities for exchange, and I want to thank the CPPA board staff for your hard work, and for the opportunity to speak today. Thank you.

**MS. HURTADO:** Thank you so much for your comment.

**MR. SOUBLET:** That was our last speaker scheduled for this morning. So I'd like to thank all of the speakers who spoke at our sessions this morning for their comments. We're going to take a break now until our next session. We'll reconvene that session at 1 o'clock, and it is on audits performed by the agency. Please feel free to leave the video or teleconference open, or to log -- log out now and then log back in at 1 o'clock for that next session. Thank you.

(Whereupon, a recess was held)

**MR. SOUBLET:** Good afternoon, and welcome back to the California Privacy Protection Agency's May 6th, Pre-Rulemaking Stakeholder Session. As a reminder, these sessions are being recorded. Speakers that are scheduled for the current session on audits performed by the agency should be signed into the public Zoom link using their name or pseudonym, and the email they provided when they signed up to request their speaking slot.

If you're participating by phone, you will have already provided your phone number that you may be

calling from, so that you may call during your pre-appointed speaking slot. Speakers will be called all in an alphabetical order by last name during this session, and we will not be able to wait if you miss your slot. When it's your turn, our moderator will call your name and invite you to speak. If you hear your name, please raise your hand when your name is called using the raise your hand function, which can be found in the reaction feature at the bottom of your Zoom screen.

Our moderator will then invite you to unmute yourself and invite you to turn on your camera if you wish. You will have seven minutes to provide your comments. In order to accommodate everyone, we will be keeping time, and if you speak for a shorter amount of time, that's okay. When your comment is completed, the moderator will mute you.

Please plan to focus your remarks on your main topic. However, if you'd like to say something about other topics of interest at the end of your remarks, you're welcome to do so. You are also welcome to raise your hand during the portion at the end of the day set aside for general public comments. Finally, you may also send your comments via physical mail, or email them to regulations@cppa.ca.gov by 6 p.m. this afternoon.

California law requires that the CPPA remain free

from using its prestige or influence to endorse or recommend any specific product or service. Consequently, during your pre -- presentation, we ask that you also refrain from endorsing or recommending any specific product or service. I now ask the stakers -- stakeholders who have been assigned to this topic to get ready to present. Please -- please use your raise your hand function in Zoom when your name is called so that our moderator can easily see you.

As noted, the moderator will call you in alphabetical order by last name. We will not move to hear comments on the topic of audits performed by the agency.

Ms. Hurtado, could you please call our first speaker?

**MS. HURTADO:** Yes. Our first speaker this afternoon is California Nevada Credit Union Leagues. Please raise your hand. Thank you. Okay, you have seven minutes to speak. Your time begins now.

**MS. QUARANTA:** Good afternoon. My name is Lisa Quaranta, vice president of regulatory advocacy with the California Nevada Credit Union Leagues. The leagues are one of the largest state trade associations for credit unions in the United States, representing the interests of approximately 250 California and Nevada credit unions,

and their more than 11 million members.

Leagues support the spirit of the law and the need to protect the personal information of credit union members, but there continues to be significant concerns with the practicality and implementation of California Consumer Privacy Act, and the California Privacy Rights Act. To that end, we thank you for providing us with the opportunity to speak today regarding the audits performed by the agency.

As financial institutions, credit unions are already among one of the most highly regulated industries. California's (indiscernible) credit unions are licensed and regulated by the California Department of Financial Protection and Innovation, and the National Credit Union Administration regulates federal credit unions, as well as federally insured state credit unions. Additionally, credit unions are subject to federal consumer financial protection bureau oversight, among others.

Credit unions currently undergo robust examinations by the regulator -- by the regulatory agencies, and which includes their -- their compliance with a plethora of privacy and data security laws and regulations. With -- with regular examinations already performed by two or even three separate agencies, plus as-needed audits performed by agencies such as Cal/OSHA, another

examination type audit performed by yet another agency, would be unduly burden -- burdensome among -- for credit unions.

A credit union's primacy regulator is better positioned to assess a credit union's ongoing compliance efforts in this area. The agency could easily defer oversight to the primary regulator. To the extent that more direct agency oversight and/or audit is deemed necessary, it would make sense for the agency to look for opportunities to cooperate and coordinate with the examinations already conducted by the credit union's primary state and federal regulator.

Because credit unions will have unique compliance issues as a result of overlapping compliance -- privacy laws, specific to financial institutions, it also makes sense to have any necessary audits performed in cooperation with the primary regulators who already understand those overlapping requ -- requirements. Additionally, due to specific exemption built into the statute for information subject to the Gramm-Leach-Bliley Act, and the California Financial Information Privacy Act, the actual compliance requirements for credit unions and other financial institutions will not look like other businesses.

As a result, it makes sense for the agency to rely

on credit unions' primary regulator that is already familiar with these requirements and exceptions. We also want to take the time to highlight other key topics separate from our primary topic for the agency's attention. Specifically, the CPRA revised CCPA's financial information exceptions to apply to personal information collected, processed, sold, or disclosed, subject to federal Gramm-Leach-Bliley Act, or the California Financial Information Privacy Act, also known as California SB-1. Regardless of this change, there's still a significant confusion regarding the exemption for personal information collected, processed, sold, or disclosed, subject to federal G -- GLBA and California SB-1.

The confusion arises because CCPA and CPRA uses terms that are inconsistent with the -- with GLBA and SB-1. GLBA and SB-1 both use terms known as nonpublic personal information and define that term to mean personally identifiable financial information. CCPA and CPRA uses the term personal information, which is defined in California civil code 1798.140(o), and is much broader than GLBA and SB-1's definition of nonpublic personal information.

In addition, GLBA pertains to personally identifiable financial information collected in the

course of a transaction or providing a financial product or service. CCPA and CPRA pertains to personal information collected basically in any manner, including when there is no transaction.

Because of the inconsistent terminology, the exemptions provided in Civil Code Sections 1798.145(e) is unclear and can be interpreted in several ways. It is essential that the agency provides clarifications in the regulations. Moreover, for financial institutions that are not only subject to CCPA and CPRA notice requirements to the extent not covered by an exception, guidance with -- with regard to the appropriate response to a consumer that recognizes this exemption would be especially useful, given that consumers are un -- unlikely to be familiar with the nature and the extent -- and to the extent with the exemptions apply.

In addition, CCPA and its regulations created several notice requirements, including notice at or before collection, right to opt out, notice of financial incentives, and updated privacy notices. Further, the regulations require specific responses to certain verifiable consumer requests. Request to know in response, and request to delete in response. CPRA added the new right, the right to request correction of inaccurate personal information, which would require a

specific response to form a verifiable consumer request -- request to correct and correct -- and response.

For all these required notices and responses, the regulations require the notices be easy to read and understand by the average consumer and provide some -- some standards to achieve that. This direction is subjective and does not contemplate a method or metric to assess the readability. Since all businesses need to provide the required notices and responses, uniform model notices would be -- would help ensure consumers understanding of the notices, simplify requirements for businesses, and create an objective review on whether a business's notices meet the standard requirements. We thank you for your time and opportunity to comment today. Thank you.

**MS. HURTADO:** Thank you for your comment.

Our next commenter is Kevin Gould. Thank you. Are you ready, Mr. Gould?

**MR. GOULD:** I am.

**MS. HURTADO:** Okay.

**MR. GOULD:** Thank you --

**MS. HURTADO:** Go ahead.

**MR. GOULD:** Thank you for the opportunity to share our perspective during this stakeholder session, which is

intended to assist with the agency's forthcoming rulemaking under the California Privacy Rights Act. I am Kevin Gould, executive vice president and director of government relations for the California Bankers Association. CBA is one of the largest banking trade associations in the United States, advocating on legislative, regulatory, and legal matters, on behalf of banks doing business in California.

The importance of protecting consumer data and privacy are not new concepts for banks, who have operated for decades under protections established by laws like the Gramm-Leach-Bliley Act, and the California Financial Information Privacy Act. As the agency prepares to issue regulations in accordance with the CPRA, we appreciate the opportunity to provide input.

With respect to the agency's authority to audit businesses' compliance with the law, we urge the agency to exempt banks, which are highly regulated and subject to ongoing supervision and frequent examination by banking regulators. Today, we are pleased to provide a very high-level overview of bank supervision and examination with a willingness to elaborate and share more detail with the agency if requested.

State and federally chartered banks already have at least three independent regulators. For example, a state

charter bank is presently regulated by the California Department of Financial Protection and Innovation, the Federal Consumer Financial Protection Bureau, and the Federal Deposit Insurance Corporation. This level of oversight includes frequent and routine examinations by regulatory agencies of not only the safety and soundness of these organizations, but of their compliance with various laws, whether focused on consumer protection, or otherwise.

Generally speaking, while the frequency of exams may vary to some degree, based on the asset size of the bank, the results of a prior examination, and the type of exam being conducted, such as a safety and soundness exam, community reinvestment act exam, or a compliance exam, the important point here is that there is a well-defined timeframe in cadence for bank examinations.

Bank examinations are comprehensive and require the bank to dedicate significant energy and resources in advance of the exam commencing. Banks are typically required to gather and compile significant amounts of records, data, and information in preparation for an examination. While examiners may conduct some portion of an exam offsite, is it typical that the regulator conducts a portion of the examination on bank premises. Examinations conclude with the regulator communicating

findings to the bank through meetings with management, and a report of examination.

With respect to the adherence to state and federal laws, banking regulators are granted broad authority when conducting compliance exams. As an example, the FDIC's consumer compliance examination manual requires the examiner to review the bank's compliance with the Gramm-Leach-Bliley Act. In this regard, the examiner is considering the bank's notices, privacy policies, internal controls, information sharing practices, complaint logs, administration of opt-out requests, et cetera.

Similarly, the California Department of Financial Protection and Innovation examine a bank's -- examines a bank's compliance with the California Financial Information Privacy Act. In furtherance of our requests that banks be exempt from audit, the agency may wish to familiarize itself with the comprehensive processes and systems that have been developed by banking regulators surrounding routine examinations, including detailed and extensive examination manuals that are publicly available. For the reasons stated, we urge the agency to consider the robustness of bank examinations, the well-developed structure that has been established around conducting exams, the extensive scope of the review

covered in an exam, and the routine and frequent nature in which these exams are conducted.

Moving to automated decision making. Federal banking regulators published notice in the federal register seeking to gather information and comments on financial institutions' use of artificial intelligence. The comment period closed June 1 of 2021. We believe the agency should refrain from applying ADS regulations to banks until federal regulators take action or should ensure that the agency's regulations do not conflict with federal requirements. Regulations should distinguish between decision making that is 100 percent automated versus partially automated with human intervention, which we believe should be outside the scope of defined coverage.

Further, if personal information is not processed through the automated decision-making technology, it should be treated as out of scope for purposes of the CPRA. The rules should exempt from the right to opt out processes that are necessary to meet legal and regulatory requirements, and processes that are operationally necessary, and where a manual process is not available.

The CPRA requires regulations to facilitate a consumer's right to correct inaccurate personal information. For regulated financial institutions, the

potential for fraud risk is a critical concern. Given extensive user authentication and identity theft prevention requirements to which financial institutions are already subject, and in light of significant risk of fraud, financial institutions should be allowed to require the use of existing channels subject to establish security and authentication protocols for any personal information correction requests.

The agency should distinguish between personal information that is active and in-use, which could be subject to the right to correct, versus personal information that is archived for record-keeping purposes and is not in use, which would be outside the right to correct.

Similarly, with respect to a business's requirement to disclose specific pieces of information, the regulations should take into consideration the challenge associated with a business accessing and retrieving archived personal information when responding to a request to disclose specific pieces of information. The agency should distinguish here again between personal information that is active and in use, which could be subject to the requirement to disclose, versus archived personal information that is retained for record-keeping purposes and not in use, which should be outside the

requirement to disclose.

The regulations should avoid overly stringent thresholds such as making such disclosures except where impossible and rely instead on commercially reasonable practices. We look forward to reviewing and commenting on draft regulations when made available. Thank you again for the opportunity to speak today.

**MS. HURTADO:** Thank you so much for your comment.

Our next speaker is Jaime Huff. Okay, Ms. Huff, hi. Your time starts now.

**MS. HUFF:** Perfect, thank you. (Indiscernible). Good afternoon, board members. My name is Jaime Huff, and I am the vice president and counsel of public policy for the Civil Justice Association of California, also known as CJAC. We're the only statewide association dedicated solely to improving California's civil liability system in the legislature, the regulatory arena, and the courts. Our membership consists of businesses and associations over a broad cross section of California industries, and we've been a trusted source of expertise and legal reform and advocacy for almost half a century.

CJAC has been asked to address the topic of audits performed by agency under the CPRA. Thank you to the agency and your staff for facilitating testimony here

today. We appreciate the opportunity to participate. CJAC believes the agency should incorporate the following overarching principles into audits performed across all identified topic areas.

First and foremost, the agency should perform audits in uniformity with global, federal, and other state standards, to avoid unnecessary complexity and burden for businesses. To the extent possible, the agency should allow audits performed by other regulatory bodies to satisfy conditions under the CPRA, which would ensure consistency with California existing laws and regulations impacting audits a wide variety of industries.

Next, the agency should recognize permanent exemptions from audits for personal information of job applicants, employees, and independent contractors collected and used solely in the context of those roles. Regular audits of such information would create undue burden for businesses. This is consistent with the purpose and intent language of the CPRA, which states that its implementation should take into account the differences and the relationship between employees or independent contractors in business, as compared to the relationship between consumers and businesses.

The audits should also not require businesses to divulge trade secrets or other confidential information

and should allow redaction of unnecessary information. The transparency goal of the CPRA would be frustrated if businesses lacked assurance that compliance with documentation and disclosure requirements will not be used against them in future litigation.

Moreover, audit information submitted to the agency should be exempt from public inspection and copying under the California Public Records Act and deemed not to constitute a waiver of any attorney/client privilege or work product protection. Addressing the scope of audits that the agency covers, CJAC believes the agency authority should be limited to specific identifiable risks, supported by evidence, prior to investigated powers being triggered.

Audits should not become phishing expeditions. They should be limited to instances where there is evidence of a business that has misused consumer information, or otherwise materially violated provisions of the CPRA. The frequency of audits should be reasonable given the time and expense businesses face to meaningfully comply with oversight. It's CJAC's recommendation that audits occur no more than once annually and should not be conducted at all until final regulations are fully adopted by the agency.

The initiation of an audit should be subject to a

majority vote by the agency board members based on evidence alleging misuse of consumer data, or a violation of the CPRA. Also, businesses should receive fair notice prior to an audit, but not less than thirty days, in order to allow for adequate preparation time. We believe businesses should have the option of selection a third-party auditor to provide an independent assessment with approval by the agency board.

Lastly, addressing the issue of safeguarding a consumer's personal information from disclosure during audits. We believe consumer data protection should be a key consideration during any audit, and the agency should provide a secure method to receive and exchange information with businesses that will not compromise said data. The agency should avoid assessing, compile -- compiling, or storing consumer data during an audit without a compelling reason. And where the agency does collect consumer personal information, we advocate for appropriate safeguards and organizational measures to protect the data. When no longer needed, the information should be promptly deleted.

CJAC believes that the adoption of these policies outlined above, auditing the agency will be cost-effective and reasonable for all parties. Thanks so much for your attention today to these recommendations, and we

appreciate the agency's effort to provide a fair and efficient regulatory framework to implement the CPRA. Thank you.

**MS. HURTADO:** Thank you so much, Ms. Huff, for your comment.

Our next speaker will be Lisa LeVasseur. Hello?

**MS. LEVASSEUR:** Hello.

**MS. HURTADO:** Ms. LeVasseur, your time starts now. You have seven minutes.

**MS. LEVASSEUR:** Thank you so much. I'm Lisa LeVasseur. I'm the founder and executive director of the Me2B Alliance, and I want to take this moment that we've changed our name to the Internet Safety Labs. We are a nonprofit product testing safe -- product safety testing organization for connected technology, and we have just published our first open safety specification for mobile apps and websites, which was several years in the making.

In addition, we have been conducting substantial research and technology audits, particularly in the K12 ad tech mobile app space for the past two years. Through the guidance and support of seasoned data supply experts like Zach Edwards, we've honed our product auditing skills and methodologies over the past few years. In particular, our audits look at safety from two key lenses. From data flow, in and out of the app or

website, and from harmful patterns, mainly of man -- manipulation and coercion in the user experience. It's based on all of this experience that we offer the following recommendations for guidance in establishing CPPA audit practices and policies. We've provided much more in-depth feedback in our written feedback from last year.

Our comments today focus on three key areas: One is the scope of the annual audits, the second is scale considerations, and the third is ethical considerations. So starting with the scope of the annual audits, primarily the ones described in Section 15, these are sort of discretionary and -- and posed to be annual audits. And we note that this -- that the language used in that Section 15, it currently refers to it as a quote/unquote, cybersecurity audit.

I wanted to just highlight that this language is probably inadequate, as cybersecurity doesn't typically relate to the full scope of what needs to be audited here. We recommend that the annual audit include auditing of privacy and safety protecting practices and behaviors beyond what is currently included typically in the scope of cyber security. Not also that when we say the privacy and safety protecting practices and behaviors, this covers both behaviors of the

organization, and behaviors of the technology itself. We're going to focus in our comments on the behavior of the technology itself, because that's our particular expertise. And we do believe that this -- that the scope of its testing really should have at its core a particular focus on independent audit of the behavior of the technology.

This annual auditing should measure the actual behavior of the technology, not just what the organization says it's doing. We recommend the scope of this auditing cover at least the three key behaviors of the technology: The data supply behavior, the harmful patterns in the UX, and the automated decision-making behavior.

When we come to scale considerations, auditing is too large a job for a single entity. It will need a network of authorized independent auditing entities. As noted in our writ -- written comments, we suggest focusing on one industry at a time, developing domain -- deep domain expertise on a particular industry, as tech behaviors needs to be understood in the context of industry norms.

I -- I want to just have one quick point on the frequency of audits. I know that the -- that the -- you know, Section 15 talks about an annual audit. I want to

just note that the behavior of technology can be changed with every single software update, and that means it could be changed every single day. So an annual only audit of technology behavior will be really woefully inadequate in order to ensure that technology is nonviolating.

Another scale consideration is we -- we want to suggest exploring and investing in the development of automated tools for detecting data flow in apps and websites. Auditing of technology we can -- we can attest to, it's a significant and labor-intensive activity. So any extent of automated tool development will be very valuable. We also suggest consideration of developing a mandatory bill of materials or ingredients labels -- ingredients label for both mobile apps and websites, to facilitate auditing.

Finally, onto ethical considerations. There's a lot of concern over -- rightfully, over preserving anonymity. These annual discretionary audits of the technology behavior, from our experience, were able to audit this technology behavior -- especially as data supply behavior -- through black box testing. Meaning, we don't need any access to internal private information, meaning there's no exposure to personal information. So when auditing the behavior of technology, you can do this

while really deeply preserving anonymity.

Much more consideration needs to be applied with ad hoc violation claims. And we did provide some more feedback in our written response on that. That -- that is trickier to preserve the -- the privacy of individuals for those ad hoc violation claims.

Finally, our final ethical recommendation is we strongly recommend that authorized auditing entities be completely divorced from industry. There can be no financial support, no affiliation with any in -- industry interest organizations. Care must be taken in ethically aligning incentives and business models for these entities, to ensure the safety and privacy of people first and foremost. Historically, industry organizations have not reliably audited for privacy and safety of their products. We simply cannot rely on them to do this. Authorized auditing entities must be independent organizations.

We're advocating for inclusivity, transparency, and accountability with the development of these authorized entities. Transparency in qualifying criteria, selection, and ongoing performance of authorized auditors, in particular publication of all of the results of these things on an ongoing --

**MS. HURTADO:** Thirty seconds.

**MS. LEVASSEUR:** -- basis. And I note that this entails annual auditor assessment evaluation.

We hope that this input is helpful, in addition to our written comments, and we look forward to hearing your thoughts in synthesis on all the comments. Thank you so much for this opportunity to share our views on this.

**MS. HURTADO:** Thank you for your comment.

Our next commenter is Daniel Magana.

Okay, we will move onto Emory Roane. Thank you. Okay, Mr. Roane, you have seven minutes. Your time begins now.

**MR. ROANE:** Excellent, thank you. Good afternoon. My name is Emory Roane, on behalf of Privacy Rights Clearinghouse and California consumers, thank you for allowing me to speak this afternoon. We are a San Diego based consumer privacy organization dedicated to improving privacy for all by empowering individuals through advocacy and education.

We look forward to continuing to engage with the agency on an ongoing basis. Our comments this afternoon are focused on a single discrete recommendation: Expanding the existing CCPA self-reporting record-keeping requirements will empower individuals, watchdog organizations, and the agency, to monitor and audit businesses for CCPA compliance more effectively.

Under current CCPA regulations and the training and record-keeping Section 999.317(g) of the California Code of Regulations, businesses that buy, sell, or share the personal information of 10 million or more consumers in a single calendar year have to annually publish CCPA metrics in their privacy policy, showing the number of CCPA requests that they've received, and how they've responded to those requests, as well as the average number of days it took for them to respond to those requests.

Now this has already given us an unprecedented though limited insight into the CCPA's impact. But it's also empowered individual researchers to identify noncompliant businesses for agency audits and enforcement. For example, we maintain multiple public interest projects at the PRC, including a database of publicly reported data brokers, and a separate database of U.S. data breaches.

Both projects rely on self-reporting transparency requirements and open data policies, to allow consumers, researchers, students, and lawmakers, to better understand the data privacy landscape and make more informed decisions. This year, Galerisom Naravi (ph.), a student researcher at Carnegie Mellon university relied on information from our data broker database and the

record-keeping requirements under the CCPA to analyze how data brokers in particular are responding to CCPA requests. He checked each data broker on our database for CCPA disclosures, assuming that data brokers, as businesses that primarily buy and sell personal information would be more likely to maintain 10 million or more individual records.

This researcher found an enormous amount of variability in the reported responses, and indications of widespread noncompliance. Of the 445 brokers that have registered with the California office, only 61 have made disclosures that are required for large data processors. Only 39 of those 61 have appeared complete and without anomalies. Thanks to those disclosures that have been made, we know that these businesses, which again, process or maintain on average, more than 10 million individual records per year, received only an average of sixty-eight consumer requests to opt out. This strongly suggests that expanding this reporting requirement would not be overly burdensome or costly, unless some broker's metrics simply don't add up, with, for example, one broker reporting that they denied 173,000 requests to opt out, though they also say they only say received 172,000 requests.

Another reports that they received 1.3 million opt-

out requests and responded to zero of them. None of the brokers studied appeared -- appeared to be properly interpreting GPP signals. We would never argue that self-reporting mechanisms are entirely sufficient, but they should be a tool in the agency's tool chest to help suggest areas of investigation. For example, while we identified 540 brokers registered across the California and Vermont offices, market research suggests that there are very likely thousands of unregistered and noncompliant marketing data brokers in the U.S. alone. One source estimated as much as 9,930 marketing technology solutions, a number up 24 percent from 2020.

We recommend that the agency exercise its regulatory and auditing authority to expand on the existing record-keeping reporting requirement, lowering the bar for required disclosures of CCPA metrics to businesses that buy, sell, or share the personal information of one million or more consumers in a calendar year. This disclosure requirement would still only fall on those businesses that collect more than ten times the threshold to be covered by the CCPA, and at the same time would provide the agency and watchdog organizations and consumers a marker of likely compliance, and an unprecedented look at the actual impact of the CCPA.

Finally, following the news that the supreme court

is poised to uproot decades of precedent and overrule Roe v. Wade, a direct attack on women's health, on reproductive rights, and on everyone's right to privacy, this agency should act to ensure that they have access to as much information as is practically helpful to protect California's privacy rights, and ensure that businesses are following their CCPA obligations. Earlier this week, VICE reported on SafeGraph, a data broker that, for 160 dollars, will sell a weeks' worth of data on where people who visited Planned Parenthood came and went before and after their visit.

Yesterday, VICE followed up that, reporting highlighting Placer.ai, a location data firm that offers heatmaps of where abortion clinic visitors live. Neither SafeGraph nor Placer.ai share any CCPA metrics on their website, and we don't know how many records SafeGraph or Placer.ai maintain. It is possible that these businesses fall outside the 10 million record bar for CCPA disclosures, but lowering the number to one million would remove any doubt.

Clearly, if any business should be making these kinds of disclosures, it should be businesses like SafeGraph and Placer.ai. And these are precisely the kind of businesses that deserve heightened attention from this auditing agency.

This agency faces steep challenges up until and after the looming deadline, and we appreciate the example demonstrated so far in its statements, staffing, and commitment to public engagement. PRC looks forward to continuing to work with this agency as you lead the state and the rest of the country into a new privacy framework. In expanding the current transparency disclosures required under the CCPA, this agency has a cost-effective, tried, and proven method, to empower Californians, and organizations like ours and others, to assist in this monumental task; to identify violators, key areas of enforcement, and areas for the agency to direct its auditing authority. Thank you.

**MS. HURTADO:** Thank you so much for your comment.

**MR. SOUBLET:** That was our last speaker for this session. We want to thank those who have already made presentations this morning and this afternoon. We're going to take a na -- a break until our next session, which just has the title of additional topics. We'll re -- we'll reconvene for that session at 2:30. Please feel free to leave your video or teleconference open, or to log out now and then back in when we join at 2:30. Thank you.

(Whereupon, a recess was held)

**MR. SOUBLET:** Good afternoon, and welcome back. It

is now 2:30, and we're about to start the additional topics discussion of the California Privacy Protection Agency's May 6th Pre-Rulemaking Stakeholder Sessions. The speakers that are scheduled to speak for the current session should be signed into the public Zoom link using the name and email they provided when they signed up to request their speaking slot.

When it's your turn, our moderator will call your name, and invite you to speak. If you hear your name, please raise your hand when your name is called, using the raise your hand function, which can be found in the reaction feature on the bottom of your Zoom screen. Our moderator will then invite you to unmute yourself and invite you to turn on your camera if you wish. You will have seven minutes to provide your comments. In order to accommodate everyone, we will be strictly keeping time. And speaking for a shorter time is just fine.

When your comment is completed, the moderator will mute you. Please plan to focus your remarks on your main topic. However, if you'd like to say something other then -- about other topics of interest at the end of your remarks, you are welcome to do so. You are also welcome to raise your hand during the portion at the end of today's session that is set aside for general public comments. Finally, you may also send your comments via

either physical mail, or you can email them to regulations@cppa.ca.gov, by 6 p.m. today.

California law requires that the CPPA refrain from using its prestige or influence to endorse or recommend any specific product or service. Consequently, during your presentation, we ask that you also refrain from recommending or endorsing any specific product or service.

I now ask the stakeholders who have been assigned to this topic, be ready to present. Please use the raise your hand function in Zoom when your name is called, so that our moderator can easily see you. As noted, the moderator will call you in alphabetical order by last name. We will now move to hear comments on the topic of additional topics.

Ms. Hurtado, could you please call the last -- or the first speaker?

**MS. HURTADO:** Okay. Our first speaker for this session is Alessandro Acquisti. Thank you. Okay, Mr. Acquisti, you have seven minutes to speak. Your time begins now.

**MR. ACQUISTI:** Thank you. I'm grateful to the agency for this opportunity. I'm an economist who studies privacy and consumer decision making surrounding privacy. I would like to make two points today. The

first concerning the economics of data privacy, the second concerning data -- dark patterns, and behavioral interventions in the privacy space.

Point one: Current economic research under the privacy is useful but insufficient. A majority of research in my own field, that is a majority of economic work and privacy, tends to focus on the economic effects of privacy regulations, such as GDPR, or in fact the California Consumer Privacy Act. While this work can be useful, there are numerous reasons why it's incomplete and insufficient, including the fact that much of this research focuses on the few and narrow quantifiable effects of regulation, missing the broader importance and significance of privacy protection.

Today, I would like to focus on one particular reason why current work in economic -- economics of privacy is being insuff -- insufficient today. By focusing on the effects of regulation, economic research in this field has not sufficiently vetted data industry claims about the purported benefits for consumers arising from inclusive tracking technology. Take online behavior advertising for instance. It is often presented by data industry as an economic win/win. A technology which benefits economically all different stakeholders. Data intermediaries, advertisers, publishers, and consumers.

There is, in fact, very little empirical validations of these claims. Very little autonomous, independent, scholarly, objective, empirical validation of these claims.

In fact, we know very little about the economic impact of behavioral (indiscernible) advertising on consumers. We do know that it reduces search costs for consumers, but search costs are just one portion of a consumer's utility or (indiscernible) function. Other elements of the function are the quality of co -- of products the consumers end up purchasing through ads, and the quality of the vendors that sell through ads. There is little to no empirical work in this area, and I encourage scholars and regulators to therefore focus their attention not just (indiscernible) study privacy impacts, on the impact, on the economic impact of the (indiscernible), in fact, focusing on what they call the allocation of economic benefits arising from data.

To the extent that the collection of data creates economic value, where does that value go? Who -- which stakeholders end up receiving value from data collection?

Point two, dark patterns is a new term for an old phenomenon, and we must pay attention to prior literature in this area. Behavior economies for over forty years have investigated how firms can use and exploit knowledge

of consumer behavior in order to influence that behavior. And this has happened in areas as diverse as gambling and dieting and physical exercises, and so forth.

Now the term dark patterns as currently used, can be certainly useful, as it can catalyze potential regulators on the way online platforms design interfaces to influence their own users. But again, research in this area didn't start in the last five years. Therefore I urge regulators to dig deeper into behavioral work on privacy that has exposed since the early 2000s consumer decision-making biases, and the decision-making (indiscernible) privacy in how platforms such as Facebook and others have taken advantage of them. A review of that body of work can be found in a piece that colleagues of Carnegie Mellon University and I published in 2017 in ACM computing surveys titled Nudges for Privacy Security: Understanding and Assisting Users' Choices Online. Thank you for this time.

**MS. HURTADO:** Thank you so much for your comment.

Our next speaker will be Cathy Gellis. Thank you. Ms. Gellis.

**MS. GELLIS:** Thank you.

**MS. HURTADO:** You have seven minutes to speak. Your time starts now.

**MS. GELLIS:** Great. Thank you. Thank you for the

opportunity to speak at these hearings. My name is Cathy Gellis, and I'm here representing myself and the Copia Institute, a think tank that regularly researches and comments on matters of tech policy, including how they relate to privacy and free speech.

I'm here today to talk about how privacy regulation and free speech converge in order to urge this board to carefully address the collision of any proposed regulation and the First Amendment, particularly with respect to the protection of speech and innovation. To do so, I want to make three interrelated points.

First, as a general matter, it is important that any proposed regulation be carefully analyzed from a First Amendment perspective to make sure it comports with both its letter and spirit. When the First Amendment says, "Make no law that abridges freedom of speech," that admonition applies to California privacy regulation. The enabling California legislation involved here itself acknowledges that it is only "Intended to supplement federal and state law where permissible, but shall not apply where such application is preempted by or in conflict with federal law or the California Constitution", and violating the First Amendment would run afoul of this clause.

It's also important that any such regulation comport

with the spirit of the First Amendment as well. The First Amendment exists to make sure we can communicate with each other, which is a necessary requirement of a healthy democracy and society. It would be an intolerable situation if these regulations were to chill our exchange of information and expression or to unduly chill innovation.

While wanting online services to be careful with how they handle the digital footprints the public leaves behind, that's admirable, the public would not be well served if new and better technologies couldn't be invented or new businesses or competitors couldn't be established because California privacy regulation was unduly burdensome or simply an obstacle to new and better ideas.

Along these lines, a second point to make is that California is not Europe. Free speech concerns do not get balanced here and cannot be balanced without violating the First Amendment. The experience of the GDPR in Europe is instructive and warning what happens when regulators try to make such a balance because invariably free expression suffers.

For instance, privacy regulation in Europe has been used as a basis for powerful people to go after journalists and sue their critics, which makes

criticizing them even more necessary, and even where under the First Amendment perfectly legal, difficult, if not impossible and best chills important discourse.

The GDPR has also been used to force journalists to divulge their sources, which is also an anathema to the First -- First Amendment and California law, along with itself violating the privacy values wrapped up in journalist source protection.

It also chills the necessary journalism a democratic society depends on, and as an aside as the journ -- journalistic of the Copia Institute has had its own reporting suppressed via GDPR pressure on search engines, so this is hardly a hypothetical concern.

And it was the GDPR that opened the door to the entire notion of "the right to be forgotten," which despite platitudes to the contrary, has had a corrosive effect on discourse and the public's First Amendment recognized right to learn about the world around them while also giving bad actors the ability to whitewash history so they can have cover for more bad acts.

Meanwhile, we have seen in Europe and even the US how regulatory demands that have the effect of causing services to take down content invariably lead to too much content being taken down. Because these regulatory schemes create too great a danger for a service if they

do not do enough to avoid sanction, they rationally choose to do too much in order to be safe than sorry, but when content has take -- been taken down, it's the world who needs it who's sorry now, as well as the person who created the content, whose own expression has now been effectively harmed by an extra judicial sanction.

The First Amendment forbids prior restraint, which means that it's impermissible for speech to be published -- punished before having been adjudicated to be wrongful, but we see time and time again such prior restraint happen thanks to regulatory pressure on intermediary services online speakers need to use to speak, which forces them -- these platforms to do the government's censorial dirty work for it by causing expressive content to be deleted and without the necessary due process for the speaker.

Then there's this next example, which brings up to my third and final point. Privacy regulation does not stay well-cabined so that it only affects large commercial entities. It is inevitably affects smaller ones directly or indirectly. In the case of the GDPR, it affected the people who used Facebook to run fan pages, imposing upon these individuals who simply wanted to have a place where they could talk with others about their favorite subject crippling burdensome regulatory

liability.

So who will want to run these pages and foster such discourse when the cost can be so high? Care needs to be taken so that regulatory pressure does not lead to the loss of speech or community as the GDPR has done, and that means recognizing that there are a lot of good online services and platforms that are not large companies, which is good. We want there to be a lot of online services and platforms so that we have places for communities to form and converse with each other. But if people are deterred from setting them up, say, their own fan sites independent of Facebook even, then that's a huge problem because we won't get these communities or that conversation.

Society wants that discourse, it needs that discourse, and if California privacy regulation does anything to smother it with its regulatory criteria, then it will have caused damage, which this agency and the public that empowered it should not suborn.

Thank you again for this opportunity to address you. A version of this testimony with hyperlinks to the aforementioned examples will be published on techder.com shortly. Thank you.

**MS. HURTADO:** Thank you so much for your comment.

Our next commenter used the pseudonym CPPA

Placeholder. I don't see them in the attendee section.

We'll move on to the next speaker, Dena Renavessen (ph.). Sorry. Dena Renavessen. Okay.

Mr. Soublet. You're on mute.

**MR. SOUBLET:** Checking one more time, is the person who used CPPA Placeholder as a pseudonym, if you're there, please raise your hand so we can hear your comments. I'll give you a minute.

Okay. And then I'll try one more time. I think it's Diana Suravessien (ph.). And of course, I'm murdering that last name, and I are really apologize for that.

Okay. Well, that was the last speaker that we had for our 2:30 session. We have one last session coming up at 3:30, which is our general public comments section. So anyone that has anything that they'd like to bring up before we close out our stakeholder sessions, please come back at 3:30.

Again, the advice would be to raise your hand, and we will call on you. At that point in time, you'll have three minutes to add comments on any of the topics that you wish. So we will take a break now and be back at 3:30. Thank you.

(Whereupon, a recess was held)

**MR. SOUBLET:** Welcome back. Good afternoon. It is

3:30 on Friday, May 6th. This is the last session of the California Private Protection Agency's May 2022 Pre-Rulemaking Stakeholder Sessions.

This is the session that is devoted to general public comments. The session is being recorded. Speakers who wish to speak should raise their hand using the raise your hand function, which can be found in the reaction feature on the bottom of you Zoom screen. They would be called in order as they appear.

When it is your turn, the moderator will invite you to unmute yourself, and then you have three minutes to provide your comments. In order to accommodate everyone, we will be strictly keeping time. When your comment is completed, the moderator will mute you.

Please note that your name and phone number may be visible to the public during the live session and our subsequent recording. If you prefer, you may also send your comment via physical mail or email them to regulations@cppa.ca.gov by 6 p.m. today.

Note, California law requires that the CPPA refrain from using its prestige or influence to endorse or recommend any specific product or service. Consequently, during your presentation, we ask that you also refrain from recommending or endorsing any specific product or service.

However, prior to moving to our general comments, we're going to accommodate one speaker who signed up for a formal time slot but was not able to confirm their speaking spot.

Mr. Christopher Oswald, we are accommodating your original request to speak on consumer's rights to limit the use of sensitive personal information. So you have seven minutes to speak now.

**MR. OSWALD:** Thank you very, very much. I certainly appreciate the accommodation and the opportunity to provide input on key topics to the agency as it drafts implementing regulations for the CPRA. Indeed, my name is Christopher Oswald, and I'm the executive vice president of government and relations at the Association of National Advertisers, the ANA.

The ANA is the nation's oldest and largest advertising trade association serving 20,000 brands of over 1500 US and international member companies, including hundreds of California-based businesses that are client-side marketers, nonprofits, and charities, fundraisers, marketing solutions providers, data science and technology companies, ad agencies, publishers, and media companies. Collectively, ANA's 50,000 industry members invest more than 400 billion dollars every year in marketing and advertising.

And I'd just like to make three quick points today. First, the ANA and its members strongly agree that protecting consumer privacy is of paramount importance. Our members have worked diligently to align their compliance programs with the CCPA's requirements and implementing regulations. At the same time, they're navigating a complex patchwork of state laws emerging across the nation. The cost borne by companies and ultimately consumers continue to rise.

One study found that state privacy law requirements could impose between 98 and 112 billion dollars of costs annually, and over a ten-year period, these costs would exceed 1 trillion dollars. The study also found that small businesses would bear an extraordinary portion of this burden, an amount between 20 to 23 billion dollars.

In the face of these astronomical costs, we urge the agency to align its regulations with other states' requirements to reduce the economic burdens of the CPRA while maintaining robust privacy protections for California consumers.

Second, the ANA and its members support responsible data practices that benefit consumers. As the agency drafts implementing regulations pertaining to sensitive personal information, we ask you to keep in mind that ordinary demographic data deemed to be sensitive personal

information under the CPRA's definition is frequently used in nonsensitive, nondiscriminatory ways that provide important benefits to consumers.

For example, the CPRA says that data that reveals a consumer's ethnic origin or religious belief is sensitive personal information. Religious organizations often seek donations from those who express interest in causes related to a particular religious affiliation. Here, the organization's intent is clear, to find people belonging to or sympathetic to a particular faith or religious denomination in order to effectively communicate with them for the betterment of the group.

Similarly, organizations of all sizes are increasingly using demographic data to inborn their diversity, inclusion, and multicultural marketing efforts as they seek to serve the many different cultural groups across our country. Additionally, various entities, including US federal agencies, have you used demographic data to target information about COVID-19 vaccines to particular constituencies.

These are just a few reasons why the opt-out approach inherent in the CPRA's right to limit the use and disclosure of sensitive personal information is the appropriate approach for the uses of such data. This structure will enable advertisers and others to reach

desired audiences with relevant goods, services, offers, and information. All of this can be achieved while still providing strong protections for consumers.

Third and finally, the agency should work to harmonize its regulations with other state laws. During the rulemaking process, we encourage the agency to carefully consider how the CCPA impacted business operations. The standard regulatory impact assessment for the CCPA found that the estimated total cost of initial compliance with the CCPA would -- was 55 billion dollars. It doesn't even contemplate ongoing costs to continue to comply where ever-changing legal requirements.

Additionally, the SRIA found that the vast majority of California businesses would be significantly impacted by the CCPA regulations. As a result, burdensome privacy CCPRA regulations could have a substantially negative impact on the ability of small, mid-sized and start-up businesses to survive and flourish in California. It's ANA's hope that the agency will strive to strike an appropriate balance between protecting consumer privacy and allowing businesses to continue to innovate, subsidize the economy, and facilitate consumers' access to a wealth of information online.

Thank you again very much for your indulgence and

your accommodation and for the opportunity to speak with you today. We certainly look forward to working with you as you promulgate these regulations, and I will be happy to submit my full testimony to the record. Thank you so much.

**MR. SOUBLET:** Thank you, Mr. Oswald.

We'll now move to the general public comment phase. Please note speakers will be limited to three minutes to provide their comments. Please raise your hand if you would like to speak.

Ms. Hurtado, could you please call our first speaker?

**MS. HURTADO:** Yes. Our first speaker in this session is Andrea Cao. Ms. Cao, you have three minutes to speak. Your time starts now.

**MS. CAO:** Good afternoon, members of CPPA board. Thank you for having us. My name is Andrea Cao, public policy manager at the California Asian Pacific Chamber of Commerce, a statewide organization dedicated to giving voice to the over 600,000 Asian-American and Pacific Islander-owned businesses in California. We're the largest statewide ethnic chamber in the state with a mission to grow and strengthen the AAPI business community.

The chamber is concerned that the CPPA has yet to

undertake the economic impact of privacy regulations as required by the law. Small businesses, particularly minority-owned small businesses, are already under significant stress, and additional regulations could heavily burden the thousands of small and minority-owned businesses in California. The businesses we represent would like CPPA to show how many API-owned businesses would be created and closed due to the CPPA regulations before any further action is taken.

While the CPRA does include an exemption for businesses that deal with data of less than 100,000 individuals, it is important to note that small businesses will still be adversely impacted. Our chamber represents a diverse array of businesses across California. We hear from larger organizations about how compliance issues will impact their ability to do business. At the same time, small businesses have made it clear that any impacts to online platforms used by small businesses will trickle down to them impacting their bottom line, for example, global out -- opt-outs making advertising less efficient and more expensive for small businesses. We know that personalized ads have been a lifeline for small businesses throughout the pandemic, helping them find new customers and grow when an act as simple as meeting in person became prohibited.

We have heard from our members that small businesses have been able to expand and better compete with targeted online advertising. We recognize the CPPA is working to get out these regulations as fast as possible, but let us not trample on innovation for the sake of expediency.

These regulations must balance critical privacy protections with impacts to large and small businesses alike, and the first step to ensure this balance is to understand the economic impact of these regulations. To date, that has -- that has not happened. Thank you for your time.

**MS. HURTADO:** Thank you so much for your comment, Ms. Cao.

Our next speaker, Julian Canete.

Mr. Canete, you may use your camera if you wish. You have three minutes. Your time starts now.

**MR. CANETE:** Thank you. Try to get on our camera here. Okay. Great. Well, good afternoon, members of the board. Julian Canete, president and CEO of the California Hispanic Chambers of Commerce. The CATC represents the interests of the over 815,000 Hispanic business owners here in California and share many of the concerns of other stakeholders regarding the economic impacts of potential regulations.

56 percent of California small businesses

experienced large, negative effects such as layoffs, missed payments, and lost revenue during the pandemic. The C -- the C -- the CPPA needs to understand the economic impacts of regulations in order to minimize additional challenges and burdens on small business.

California's small businesses have already been especially hard hit by the pandemic and cannot afford additional adverse impacts from rushed regulations. Previous comments by the C -- CPPA about how these regulations will not impact small business are simply not true. Small businesses are largely forced to pivot during the pan -- during the pandemic to conduct more commerce online, turning to online advertising and the use of digital platforms to connect with their customers. Changes to compliance requirements for these platforms will inevitably impact our members, large and small, to do business in California making online advertising more expensive and less likely to connect to key customers.

This impact may not mean much to many, but I can tell you it means everything to our member companies, especially our small Hispanic-owned businesses.

As agency proceeds with its rulemaking process, small businesses must be afforded the opportunity to weigh into the conversation in a meaningful way. It is incumbent on each of you to listen and learn about how

small businesses in California have adapted to the pandemic in our shifting economic landscape before, now -- now af -- not after a new sprawling regulatory framework is thrust upon them.

We call on the CPPA to show us with specificity how Hispanic businesses will be impacted by upcoming CPPA regulations and determine how many of -- of these businesses will be forced to close due to adverse impacts. Thank you for the opportunity.

**MS. HURTADO:** Thank you so much, Mr. Canete, for your comment.

Our next speaker will be McKenzie. Okay. Ms. McKenzie, you have three minutes. Are you there?

**MS. MCKENZIE:** Yes. Sorry.

**MS. HURTADO:** That's okay. You have three minutes. Your time starts now.

**MS. MCKENZIE:** Okay. Good a afternoon, Chair and members of the board. Thank you for this opportunity to speak. My name is Zanamoris (ph.), and I am a small business owner of the Pam Firm located in Long Beach, California. My business, like the other 1.2 million minority-owned small businesses across the state, continues to feel the effects of years of uncertainty and repeated closures caused by the pandemic and exacerbated by inflation and supply chain disruptions.

Digital platforms have become more important than ever to our daily operations. During the COVID-19 health crisis, we have used social media to advertise and communicate directly with customers, continue virtual administrative support, and ultimately keep or doors open, but CPPA missing the statuary deadline of July 1st, 2022 set by Prop 24 carries a significant financial burden and risk for my business and my customers. Small businesses like mine are too important to our economy to not have significant input in the rulemaking process.

What is the Board doing to engage small businesses and make sure we are part of this process? We are working every day to keep our doors open and cannot afford to spend or time monitoring CPPA's website for updates.

There are our four million small businesses in this state. How many have you reached out to? Small business owners want the best for their customers, and that includes protecting their privacy while conducting business online, but our voices should be essential to this process and can help ensure regulations are practical and reasonable. By reaching out to our communities, we can get this right for businesses and consumers. Thank you for your time.

**MS. HURTADO:** Thank you so much for your comment.

Just one moment. Our next speaker, Dazza Greenwood.

Mr. Greenwood, you have three minutes to speak. Your time begins now.

**MR. GREENWOOD:** Great. Thank you very much. I am Dazza Greenwood. My company is CIVICS.com. I should ask, how is my audio? Is it coming through?

**MS. HURTADO:** Your audio is fine, but your video is --

**MR. GREENWOOD:** Oh.

**MS. HURTADO:** -- the wrong way. There you go.

**MR. GREENWOOD:** The consumer product definition of orientation for screens, I guess.

**MS. HURTADO:** Certainly.

**MR. GREENWOOD:** So thank you for that. I -- I wanted to make some brief informal comments about the role of open standards and you know, I'm aware that there are more than one standards efforts afoot now that would help businesses and consumers alike to -- to actually conduct interactions under CCPA and -- and the related law, and I would like to encourage the AG's office and the other regulatory bodies that are coming online soon to really embrace the open standards processes and to look at how the outputs of these standards can help to -- to fill out the toolkit for implementation of the statute.

And in particular, I think some comments earlier in this process in the previous days have -- may have suggested looking at some open standards as mandatory. I'd like to also suggest, you know voluntary standards are very important to consider, and one way to connect them to mandatory regulation would be as a voluntary safe harbor, perhaps, to the extent that a standard is deemed by the regulator to mead or exceed the regulatory requirements as an option for businesses and consumers alike to adopt in order to comply with the regulations.

So that's the -- that's the emphasis of my contribution. I hope that you'll continue to really support and reflect the standards efforts and to embrace and adopt them as regulation continues to evolve. Thank you.

**MS. HURTADO:** Thank you so much for your comment, Mr. Greenwood.

Our next commenter is Chris Frascella. Just one moment.

**MR. FRASCELLA:** Good afternoon, and thank you for the opportunity to comment. My name is Chris Frascella with the Electronic Privacy Information Center, and I'm offering a comment about fraudulent emergency data access requests.

So on March 29th, Brian Krebs published an article

about hackers successfully obtaining personal data through fake emergency data requests, for example, by forging court documents or by compromising legitimate law enforcement email accounts. On April 26th, Bloomberg published on article on child victims of this practice. Bloomberg reported that Facebook, Apple, Google, and Snap are among the companies that have voluntarily given hackers consumer data.

Reports suggest that due to the alleged emergency, tech companies do not wait to verify the data access request with the impersonated law enforcement agency. The company merely notices that the email came from a law enforcement email domain and hands over the consumer's personal data to the hacker.

The guardrails on emergency data access requests in Section 1798.145(a)(4) of the CCPA pertain to protecting against civil liberties abuses by government agencies. Because these guardrails are centered on internal agency determinations and commitments, they do not apply meaningful against fraudsters.

We ask, how can the agency protect consumer data from these attacks, which are only as successful as tech companies' policies and practices permit. In July of last year, Senators Wyden, Tillis, and Whitehouse introduced a bill that would require courts to use

encrypted digital signatures to combat the use of counterfeit court orders. At the agency's March 30th meeting, Professor Christopher Nagle discussed requiring companies to internalize the risks of data collection, such as cybersecurity failures.

We propose the agency clarify that companies cannot rely on the emergency access exception unless law enforcement organizations provide separately authenticated verification of emergency data access requests and that the agency require companies receiving emergency data access requests to utilize said authentication method or to verify the request validity, not by replying directly to the apparent request sender, but instead by contacting a law enforcement organization from which the request seems to have come. A company should not be able to avail itself of the 145(a)(4) exception if the company fails to comply with this requirement. Thank you.

**MS. HURTADO:** Thank you so much for your comment, Mr. Frascella.

The next speaker is Elexix Carmichael

All right. Elexix Carmichael, you have three minutes. Your time begins now.

**MS. CARMICHAEL:** Good afternoon. My name is Elexix Carmichael, and I am the co-owner of SAGE Carpet Cleaning

Business and Upholstery Services in San Bernardino County. I'm concerned about the lack of input from minority-owned business leaders like myself in the stakeholder process. Every morning we take to monitor this week's stakeholder meetings is time taken away from serving our customers and taking care of our employees.

The COVID-19 pandemic has put us through the ringer, but we were able to use social media to communicate directly with our customers to stay in business. I also advertise online to reach perspective customers and to build my business' reputation in the community.

Protecting the privacy of my customers is critical and important, and I respect the efforts being made to ensure the privacy of all Californians is protected, but it is also important that small businesses like mine, which are the backbone of the economy, can compete and survive. Sorry. I got muted again.

There must be a balance between these two important priorities, and the CPPA has itself acknowledged the importance of striking this balance. Not all business owners are able to take time away from their day-to-day operations to log onto three days of stakeholder meetings to ensure that their voices are heard as the CPPA puts together these crucial regulations.

The CPPA needs to do more it to reach small business

owners where they are. These regulations will drastically impact how we do business, and we should have a seat at the table in establishing fair, equitable, and practical regulations. Thank you so much for your time.

**MS. HURTADO:** Thank you very much for your comment.

Our next commenter is Edwin Lombard.

Okay. Mr. Lombard, you have three minutes to speak. Your time begins now.

**MR. LOMBARD:** Thank you, Chair and members of CPPA. I made public comment earlier this week on the 4th, and I just wanted to follow up on that. I continue to be amazed at the lack of black-owned small businesses that are aware of, number one, your organization and this very crucial piece of regulation that is being formed that's going to have a devastating effect -- can potentially have a devastating effect on how they do business in the state of California.

I'm a concerned small business owner, and just yesterday I was at my barber's getting my hair done, and I had a conversation with him about who you are and what you are actually doing, and he became very upset with the fact that he had no idea that this was taking place, and he's a very active person when it comes to legislative and regulatory issues because the barber shop in the black community is -- is one of the main communication

points when it comes to these types of issues.

And the comment that he made to me was, he said, don't they realize that when corporate America catches a cold, that we small business owners catch pneumonia? So the effect that you can potentially have on large corporations and large businesses may seem minimal, but it can be a devastating effect that it's going to have on black small businesses throughout the State of California.

So I ask number one, that you come up with a better way to outreach to black small businesses and also be very careful about how you write this regulation and make sure that our businesses are considered in the process. We definitely would like to have a voice in this and -- and would like to be able to make public comment whenever we can. Thank you so much.

**MS. HURTADO:** Thank you, Mr. Lombard, for your comment.

We have one more hand raised. Kaitlyn Johnson. Okay. Kaitlyn Johnson, you have three minutes to speak. Your time begins now.

**MS. JOHNSON:** Great. Hi. Good afternoon, everyone. Can you hear me all right?

**MS. HURTADO:** Yes.

**MS. JOHNSON:** Okay. Perfect. So on behalf of

California Water Association, we're providing these comments on the proposed regulations concerning the CCPA. CWA is the statewide association representing the interests of water utilities subject to the jurisdiction of the California PUC. CWA's members provide safe, reliable, high-quality drinking water to approximately six million Californians, and we appreciate the opportunity to comment on the proposed regulations and assist in providing greater clarity to businesses and consumers with respect to CCPA implementation.

On the topic of consumer rights to opt out. The CPUC has authorized water utilities to release customer-specific information to local governments, wholesale water agencies, and other entities for the purpose of calculating local taxes, managing wastewater systems, collecting miscellaneous fees, and implementation and enforcement of conservation programs and measures.

The transfer of this customer-specific information best serves important public policy interests. The CPUC has established (audio interference) of the customer information that is shared is kept private and only used for the purpose for which it is intended. Although some water utilities may collect a nominal fee related to the transfer of data to a neighboring municipality or

wastewater utility, they do not sell data in the manner for which the CCPA was designed to provide protection.

The fees collected by the water utilities simply place the financial burden and cost of accumulating and transferring the data onto the party requiring the information rather than the utility -- utility's customers. The opt-out provisions in the CCPA and the proposed regulations should not apply to this type of data collection and sharing by water utilities since the information is not being used for commercial purposes, but instead to serve the public good.

On the topic of consumer right to delete. CPUC General Order 103-A established minimum standards for design, construction, location, maintenance, and operation of the futilities of water and wastewater utilities operating under the jurisdiction of the PUC. General Order 103-A also sets forth requirements for record retention.

Pursuant to the general order, certain records, which include records containing personal customer information, must be retained for at least ten years and longer in certain circumstances. In order to comply, water utilities are not in a position to grant customer requests under the CCPA to delete customers-specific information unless the information was no longer required

to be retained by the CPUC.

**MS. HURTADO:** Thirty seconds.

**MS. JOHNSON:** At this point, these records may have been moved to offsite storage or maybe in difficult-to-manage forums such as tape logs. The burden of locating and deleting these records would far outweigh any public benefit. CWA therefore requests that historical water utility records more than ten years old be exempt from deletion request obligation. And I will close with that. Thank you very much.

**MS. HURTADO:** Thank you for your comment.

Mr. Soublet, there are no more hands raised. We'll give it a minute if someone wants to raise their hand.

**MR. SOUBLET:** I'd like to wait one minute to see if there's anyone else who would like to raise their hand and make some general public comment. So -- so we'll wait until 4 o'clock before we make our concluding comments.

Okay. I want to thank you everyone that participated in our sessions this week. As you know, we know we have a task of working on the regulations that we've all commented upon.

Before we close out, I'd like to turn it over to our executive director, Ashkan Soltani, to make some concluding comments.

**MR. SOLTANI:** Thank you, Brian.

Good afternoon, everyone, and thank you all for participating in the CPPA's May 2022 Pre-Rulemaking Stakeholder Sessions. I want to express my sincere gratitude to all the stakeholders that took the time to provide comment over these last three days. We truly appreciate the diverse voices that have been -- that have participated as the -- and provided the perspectives offered.

As the chairperson mentioned at the beginning of the program, these sessions mark the third of our pre-rulemaking activity, which began last year. We had an -- we had an incredible interest in these topics and hope that stakeholders continue to engage in these forums when we embark on our formal rulemaking.

If you would like to submit written comments and haven't already, please submit your comments to us a regulations@cppa.ca.gov by 6 p.m. today. Stakeholders' comments, along with the transcription recordings of these sessions, will be posted on our website under the meetings and events page once they've been processed.

I'd also like to thank our team from CCPA -- CPPA and the Office of the Attorney General for supporting us today.

Mr. Brian Soublet, who is hosting, and Ms. Trina

Hurtado, who is acting as moderator, thank you both for all your time over these three days.

I'd also like to thank Ms. Stacy Hyacinth (ph.) for administrative staffing, and additionally, I'd like to generally thank the staff at Businesses Consumer Service and Housing Agency, BCSH, and the Department of General Services, the Office of the Attorney General, and other agencies who helped us behind the scenes.

Thank you all for joining us today, and thank you all for helping support us. This concludes the May 2022 stakeholder sessions of the California Privacy Protection Agency. Thank you.

(End of recording)

TRANSCRIBER'S CERTIFICATE

STATE OF CALIFORNIA )
)
COUNTY OF SACRAMENTO )

This is to certify that I transcribed the foregoing pages 1 to 112 to the best of my ability from an audio recording provided to me.

I have subscribed this certificate at Phoenix, Arizona, this 7th day of June, 2022.

DeEtte Hicks

eScribers, LLC

--o0o--