AMENDED TRANSCRIPTION OF RECORDED STAKEHOLDERS SESSION

OF CALIFORNIA PRIVACY PROTECTION AGENCY

MAY 5, 2022

VIA TELECONFERENCE

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

Transcribed by: Cynthia R. Piett,
eScribers, LLC
Phoenix, Arizona

--o0o--

**AMENDED TRANSCRIBED RECORDED PUBLIC MEETING**

**OF CALIFORNIA PRIVACY PROTECTION AGENCY**

**May 5, 2022**

**MR. SOUBLET:** Good morning. Welcome to Day 2 of the California Privacy Protection Agency's May 2022 Pre-Hearing Rulemaking Sessions. My name's 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 sign up. This event, the stakeholders' sessions, is the agency's third pre-rulemaking activity. While subcommittees of the board provided input to 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 and I will go over the plan for this session. First, let me sketch the format of the stakeholders' sessions so everyone has a sense of how things will proceed. As you can see from the program and schedule, which you can find on the meeting and event page of our website, we are holding a series of stakeholder sessions this week, yesterday, today, and tomorrow, 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 which will be limited to seven minutes. We will proceed through the program according to the schedule provided on the website. Please note that all 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'd 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, you will have an opportunity to speak during the time set aside for general public comment at the end of each day. Please take a moment to review the schedule to see when the public comment is expected to occur. And again, please note that the times are approximate. Each speaker making general public comments will be limited to only three minutes. We will strictly keep time for all speakers in order to accommodate as many stakeholders as possible.

Speakers that are scheduled for the current session should be signed up into the public Zoom link using the name or the pseudonym and email that they provided when they signed up to request their speaking slot. If you

are participating by phone, you will already have provided the phone number that you will be calling from so that we may call on you during your pre-appointed speaking slot.

Note that your name and phone number may be visible during the public session and in the subsequent recording. Speakers will be called in alphabetical order by last name during this window and we will not be able to wait if you 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 screen.

Our moderator will invite -- 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 than the 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.

Finally, you may also send us your comments via physical mail or email them to regulations@cppa.ca.gov by Friday, May 6th at 6 p.m. California law requires that the CPPA reframe 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 that stakeholders who have been assigned the topic of data minimization and purpose limitations to be ready to present. Please use the raise your hand function in Zoom when your name is called so that our moderator can see you easily. As noted, the moderator will call you in alphabetical order by last name.

We will now move to the comments on the topic of data minimization and purpose limitations.

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

**MS. HURTADO:** Yes, good morning. Our first speaker today will be Stacey Gray.

Stacey Gray, can you raise your hand, please? Thank you. Ms. Gray, you have seven minutes. Your time starts now.

**MS. GRAY:** Thank you so much. Good morning. Thanks -- thank you to the agency for the time today. My name is Stacey Gray and I'm the director of legislative research and analysis of the Future of Privacy Forum.

FPF is a global nonprofit that focuses on consumer privacy and law with a particular focus on emerging technologies. We work with chief privacy officers of companies across all sectors as well as scholars, academics, advocates, and policymakers to help drive consensus around principle business practices for emerging tech.

I'm here today, this morning, to offer a few thoughts on the principle of purpose limitation. The California Privacy Rights Act requires businesses to disclose the purposes for which the PI they will collect will be used and prohibits them from collecting additional categories of information or using the personal information collected for additional purposes that are "incompatible with the disclosed purpose for which the information was collected without additional notice." That's from 1798.100.

As a general business obligation, this reflects the principle of purpose limitation in the Fair Information Practices. So I'll keep this brief. My testimony today is intended to, first, simply encourage the agency to

engage in rulemaking on this issue to the extent that it can devote resources to it. And secondly, to offer a few recommendations on what might be considered compatible versus incompatible business practice.

So first, under section 185, the agency has a general mandate to issue regulations with respect to defining business purposes for which covered entities may use PI consistent with expectations. We'd encourage the agency to specifically exercise this authority to provide guidance on what is considered incompatible under 1798.100(a)(1).

So why? Purpose limitation is a fundamental principle to the Fair Information Practices. It protects individual and society -- societal privacy interests without relying on individual consent management. So that's a key -- key thing. It protects against a -- a core type of privacy violation which is covered entities collecting data for one purpose, using it for a very different one.

We see numerous examples of such violations in recent years, some of them enforced by the FTC as the amount of data available for consumer devices has grown. For example, an individual may consent to sharing precise persistent location information with an app or a service in order to obtain a specific consumer product or service

like a weather alert, unaware that that data might be later sold and shared for very different incompatible purposes such as anything from simple monetization to sharing with law enforcement.

Given the importance of this principle, the agency should ensure not only that its respected by covered entities but also consider providing robust guidance on -- on it for the purposes of clarity for both consumers and businesses.

Incompatible secondary uses of information should be interpreted strictly. They should include those not reasonably expected by the average person. For example, invasive kinds of advertising profiling unrelated to providing a product or service requested by the consumer, training high-risk algorithmic systems such as facial recognition, or voluntary sharing with law enforcement.

At the same time, the agency should consider publishing guidance and clarity for businesses on what might be considered a compatible secondary use of information. Some secondary uses of information can include scientific, historical, or archival research that is in the public interest. When subjected to appropriate privacy and security safeguards, this kind of secondary use of information, which may or may not be contemplated at the point of collection, can lead to true social

benefits such as public health tracking.

Many companies can induce, successfully partner with academic institutions to share information for purposes for conducting such research. It's often on a limited or modified data sets and under contractual limitations, sometimes under IRB oversight from an affiliated institution. There are many reasons companies may be cautious about this, and one of those might be, you know, not understanding what is considered an incompatible use. But in addition to trust, reputational risk, companies are navigating complex legal and policy questions related to this type of secondary use.

So I will -- I will stop there and just encourage the agency to consider scientific, historical, and archival research that is in the public interest to be considered a compatible secondary use of information, in addition to providing case studies for businesses and consumers and interpreting the provisions strictly to ensure that this very important principle of the Fair Information Practices is respected.

So thank you for your time. Happy to follow up further with additional resources. And I -- I'll stop there. Thanks.

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

The next commenter will be Eric Null. Eric Null,

please raise your hand. Thank you. Okay. Mr. Null, you may use your camera if you wish. Your time, seven minutes starts now.

**MR. NULL:** Thank you. Thank you for allowing me to speak to you today on data minimization and use or purpose limitations. I'm Eric Null. I'm the director of privac -- the privacy and data project at the Center for Democracy & Technology, which is a D.C.-based nonprofit, nonpartisan organization that is committed to protecting privacy as a fundamental human and civil right.

Data minimization and purpose limitations are critical data protection principles that are often overlooked and not taken very seriously in the U.S. Many businesses set their own data agendas, crafting essentially limitless practices and dense privacy policies. And businesses often don't think critically about their data practices nor try to limit the potential data-related harm that they can cause.

Data's a commodity prone to over collection. A survey of industry leaders in the U.S. showed that 36 percent of them believe that over three-quarters of their data is dark, which is essentially unused data, and sometimes it's not even known that they have it and 63 percent of them believe that over 50 percent of their data is dark.

A recently leaked document from Facebook shows that the company has no idea where all of its user -- user data goes and what it's doing with it, which make -- which would make it seemingly difficult to comply with the EU's general data protection regulations own data minimization and purpose limit requirements. And one broader EU study showed that 72 percent of companies collected data that they didn't end up using.

Anecdotal examples of over-collection exists as well. Mobile apps like Angry Birds and the infamous Brightest Flashlight app have had a history of collecting location data without a legitimate purpose. Data brokers who exist in significant part because of data overcollection and retention have in particular capitalized on this trend. Just this week we saw reports of a data broker selling location data of people who visited Planned Parenthood clinics. That the broker -- the broker then collecting that information using software development kits from various mobile apps that track location for who knows what reason. And we also learned today that one data broker made that same location data available for free.

And several years ago, mobile carriers were caught providing cell-site location data to third-party data broker -- data brokers that ended up in the hands of

bounty hunters. For their part, people don't want companies to collect such extension data about them. A 2020 survey showed that almost 80 percent of Americans expressed concern over sharing personal information with online businesses. And in 2019, a significant majority of peer survey respondents were concerned about how much data about them is collected by businesses, and similar numbers believe the risks to such data collection outweighed the benefits.

Data minimization and purpose limitations are potential solutions to these problems. At its strictest, the minimization principle requires companies to collect only the data they need to provide the product or service and nothing else. But many definitions like Californias are broader and tie minimization to specific purposes or uses. These are important substantive provisions in the CPRA and I encourage your agency to engage meaningfully with the plethora of uses for which companies collect data and decide whether there are harmful uses that require curtailing or limiting.

One approach taken by my organization, CET, and its comprehensive privacy framework a couple years ago was to prohibit certain harmful data practices when those practices are -- were not required to provide or do not add to the functionality of a product service or specific

feature that a person has requested. Those practices include biometric tracking, precise location tracking, cross-device tracking, tracking their children under thirteen years of age, collecting the content of or parties to communications, audio, and visual recording, or -- and health information. These uses, when employed beyond the functionality of the product or service, can cause harm without countervailing benefits and they should be limited.

In addition to that list, I would encourage your agency to clarify and limit secondary data use. As Ms. Gray mentioned, the CPRA states that companies can collect data that is reasonably necessary and proportionate to achieve the original purpose of the collection or another disclosed purpose that is compatible with the context in which the personal information was collected.

This language makes clear that the importance of disclosing essentially all uses and it disallows many secondary uses already. And then any additional secondary uses are limited to only those that are compatible with the context of the original collection, meaning there must be some direct connection between the secondary purposes and the original purpose.

So for instance if a business collects a person's

phone number for account verification purposes, it could not then -- then later use that data to serve ads because that is a wholly different context and would be incompatible with the original collection.

I would encourage your agency to also limit discriminatory data use. We know that data can be used to discriminate both directly and through algorithmic discrimination.

Years ago, the U.S. Department of Housing and Urban Development sued Facebook for letting housing advertisers filter out -- filter out ad users on the basis of their race, color, religion, sex, familial status, nationality, or disability. Amazon previously used an HR recruiting tool that downgraded women on the basis of their gender because Amazon's training set for the software included resumes from mostly men.

Under no circumstances should companies be allowed to use data or train algorithms in ways that discriminate against people based on protected characteristic, particularly in housing, credit, employment, insurance, and education. And I'll say one final note on the forum. We all know that privacy policies are poor vehicles for informing people about actual data practices. People don't read them. They're too long and difficult to read. And even those who do read them will find a confusing

laundry list of practices a business may, quote/unquote, may engage in, and without -- so without describing actual practices, it's almost impossible to understand what data businesses have about people and how it is used. The agency should clarify that businesses should create easy-to-read summaries that describe the most salient data practices that businesses actually engage in.

And with that, I thank you for the chance to speak to you today and I look forward to working with the agency.

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

Our next speaker is Sophie Stalla-Bourdillon. Thank you. Okay. Ms. Stalla-Bourdillon, your time starts now. You have seven minutes.

**MS. STALLA-BOURDILLON:** Thank you. Thank you so much for the opportunity to speak. I am Sophie Stalla-Bourdillon, senior privacy counsel at Immuta, which is a software company (indiscernible) governance tools and privacy (indiscernible) technologies, and professor of technology law and data governance at University of Southampton UK.

So a few thoughts on purpose limitation and data minimization. These have been criticized for being (indiscernible) driven business models such as those

based upon providing purpose limitation and data minimization and decision making. An argument against purpose limitation and data minimization state that it's not possible and it's not even desirable to pursue data minimization. In particular, in the context of the (indiscernible), (indiscernible) learning, and AI. In particular, if one is serious about innovation. That said, the principle have been reaffirmed within leading standards such as GDPR, and emerging in U.S. state law we've had CCPA, CPR with (indiscernible) of GTs, and definitions of business purposes.

The claim that I like to make here is that purpose limitation and data minimization are core safeguards, so I'm echoing other speakers as much as the identification techniques if not more. And this is true for three fundamental reasons. First, the legitimacy of the processing can only be derived from the processing purpose not from the data identification technique that is applying on the data. The identification only mitigates against consents related to confidentiality and privacy is much more than the protection of the confidentiality of the information. And this is true even if individuals do not raise objections against the processing. As been said, that's consent is not the best way to protect individuals in that space.

Second, the identification, in fact, implies purpose limitation and data minimization. Why? Because the identification is risk-based. Zero risk cannot be guaranteed. And in practices what we see is that purpose limitation and data minimization are used as best practice for identifying data, in particular, (indiscernible) base to do (indiscernible) determination, for example.

And even to try to meet the CCPA identification test, purpose-based access control and monitoring here is the key. And finally, (indiscernible) processing activities obviously will not require -- will require processing in plain text in the clear, therefore the identification is not always an option.

In my work, I've tried to show that it is possible to reconcile purpose limitation and data minimization and they are driven activities by adopting a dynamic approach to purpose limitation and data minimization and distinguishing between (indiscernible) purposes and decision making. In particular, individual decision-making. And this research work has been confirmed by my experience in the industry. If you just take an example, the (indiscernible) for example, that is being used to build the architectures, it forces an organization to organize the activities by problem spaces, so they are

good signs or so within the industry.

The CCPA standards for purpose limitation and data minimization appear below what we have in the GDPR, which is not (indiscernible) guidance has been issued on GDPR has always been very clear. The question is therefore whether more specificity should be required in order to make data minimization more meaningful, or whether requiring more specificity for purpose limitation would be self-defeating and would undermine innovation.

I'll be clear, pushing for more specificity is good practice to be able to better anticipate individual harm and achieve a higher degree of data minimization, which is actually a requirement also for (indiscernible) only, as long as purpose limitation and data minimization principles are understood dynamically. In other words, purposes can be and should be refined of a time just like the amount of data that is being processed to pursue these purposes.

How do we achieve more specificity? If you look at GDPR for example, they -- through their distinction between legal basis and purposes, they try to push for more specificity. This is not the only way to do it. There are other ways. In particular, the distinction between legal basis and purposes can be confusing, but this does not mean that it's not possible to push for

more specificity. And in fact, I would encourage the agency to seriously consider different ways to incentivize more specificity. As other speakers have been saying earlier, strict interpretation of the requirement of compatibility of purposes is -- is one way to do that.

To require more specificity and privacy notices even if they are not very often read by users, this is -- this is -- this is a starting point. This is forcing organizations to think about their processing activities. To require more specificity or so within the recording obligations can make a difference and to impose risk assessment obligations in which purposes and sub-purposes can then be unpacked.

And with this, I -- I -- I -- I -- I finish my speak. I thank you to the agency. I'm happy to -- to continue to engage with their work. Thank you.

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

**MR. SOUBLET:** Thank you. That was our last speaker that was signed up for this session. So I want to thank everyone that spoke so far this morning.

We're going to take a short thirty-minute break until our next session which is on dark patterns. We'll reconvene for that session at 10 o'clock. Please feel free to leave the video or teleconference open or to log

out and back in at 10 o'clock when our session on dark patterns resumes. Thank you.

(Whereupon, a recess was held)

**MR. SOUBLET:** It's now 10 a.m., and I'd like to welcome you all back to the California Privacy Protection Agency's May 2022 Pre-Rulemaking Stakeholders Sessions. I would also like to remind you that the session is being recorded. Speakers that are scheduled to speak during this current session on dark patterns 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. Speakers will be called on in alphabetical order by last name during this window 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 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 for a shorter 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're also welcome to raise your hand during the portion at the end of the day that we've set aside for general public comments.

Finally, you may also send us your comments via physical mail or email them to regulations@cppa.ca.gov by 6 p.m. Friday. California law requires the CPPA to 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 reframe from recommending or endorsing any specific product or service.

I now ask the stakeholders who have been assigned the topic of dark patterns to 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 dark patterns.

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

**MS. HURTADO:** Yes. The first speaker for this

session is Amy Allshouse.

Thank you. Okay. Ms. Allshouse, your time will be seven minutes. It starts now.

**MS. ALLSHOUSE:** Thank you. Thank you for this opportunity to share my thoughts on dark patterns. I am a second-year law student studying privacy law and I have been a web developer for over twenty years. I would like to encourage the agency to engage in rulemaking and give guidance to businesses and other online entities on dark patterns. This is about valid consumer consent. In essence, not tricking people, both in relation to getting people to give their data and to make purchases.

The purpose behind dark patterns regulations is to ensure that online entities cease using misdirection, confusion, or psychological manipulation to gain data or complete transactions. Regulating dark patterns will help consumers and businesses by creating an online environment with less uncertainty and more safety.

I'll briefly talk about four dark patterns that I request the agency regulate and I'll explain briefly what I mean by each practice. I'll talk about overt deception, hidden costs, forced continuity, and the most important category, deceptive designs. Overt deception means inducing action based on false beliefs. So a false countdown timer or the indication that there's only one

item left when that's not the case.

Hidden costs mean hiding the real purchase price until the checkout page and in some cases, maybe where services are provided. This can even happen after checkout. Forced continuity is usually a free trial where credit card information is required and then there is no reminder to cancel before the free trial is over and the consumer automatically begins paying, or it is just incredibly difficult to cancel a service.

Finally, deceptive design. I would suggest we adopt this language to refer to dark patterns instead of calling them dark patterns because deceptive design is a clearer way to refer to these practices and can be more universally understood.

So deceptive design is anything that serves to trick or confuse. It can be as simple as making one option prominent and another option hidden, but it's any decisi -- it's hard to say this -- it's any design decision that psychologically manipulates the consumer or a site visitor. And essentially, these practices -- all of these practices have no place in a healthy online world.

The core value in regulating here is transparency which I will -- which I believe will be better not only obviously for consumers, but for all -- for online

entities in general, businesses, and others alike because it will raise the quality of online experiences overall.

Thank you very much.

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

Our next commentor will be Cassia Artanegara. Thank you. Okay. Ms. Artanegara, you have seven minutes. Your time starts now. You may use your camera if you wish.

**MS. ARTANEGARA:** Hi. Thank you for inviting me to speak. My name is Cassia Artanegara speaking on dark patterns. I'm a UX Designer and program manager at a program called DataCurious whose mission is to empower individuals and communities to make informed decisions about their data.

I have a background in computer science and art and my work revolves around researching, designing, and communicating better relationships between humans, the data we produce, and the entities that use that data.

I speak today as an advocate for what an issue typically calls users and consumers. And my work centers of humanity of these people who are exploited by a system of entities prioritizing profit over people.

I won't get into all of that but I urge you to make three calls -- calls to action today. One is to clearly define dark patterns; two is to provide examples of good

and bad privacy controls; and three is to shift the burden of responsibility from users to companies by restricting how companies can collect, use, and profit from data.

Now I'll expand on those three calls to action. So the first, we need to define dark patterns more clearly. The current CCPA definition defines a dark pattern as a user interface designed or manipulated with a substantial effect of subverting or impairing user autonomy, decision making, choice as further defined by regulation.

This is a great starting point but this definition needs to be expanded to identify the specific dark patterns that might influence a person to make a decision that they didn't need to make or is harmful to their well-being. An example of this is -- you know, I'm sure you've seen in cookie consent banners how prominent the accept button is styled, so it's bigger, bolder, brighter, and the reject button is not as visible.

And this can also be as subtle as a choice in the words that's used that implies that a user has already given consent which can then prime them to consent.

Additionally, the specific context for a dark pattern may appear, need to be called out. So when you think about the last app that you used or the last website you used, there are so many decisions that you've

made throughout your engagement with that app that might be touched by a dark pattern. An example is deceptive marketing that kind of positions as an app as one thing when its true purpose is to collect data about their users. And that deceptive marketing can influence you to download that app without really knowing the full consequences of that.

I do want to call out that dark patterns aren't necessarily always malicious, sometimes they're just a result of sloppy or thoughtless design. And so actually calling them out explicitly can help companies avoid accidentally using dark patterns, and also encourages companies to provide privacy controls that affirm humanity and agency.

The second call to action is to provide concrete examples of good and bad privacy controls. There aren't many examples of really great privacy controls, nor are there specific standards or regulations. And we can elevate that standard or define that by saying explicitly, like, here's what that looks like, rather than waiting for a company to, you know, get there on their own. That would be a really valuable resource for companies especially smaller ones who are navigating and trying to adapt to changing privacy regulations.

I do also acknowledge that explicitly prescribing

those examples could hinder more entrepreneurial innovation or even be rendered obsolete in two years when we have the next new -- the next new technology. So that is something that needs to be balanced and navigated in the future.

So far, I've made two recommendations to explicitly define dark patterns and to call out the context in which they appear, but these are simply not enough. Consumers should not have the burden of navigating harmful and exploitive data practices. The burden should be on companies and they shouldn't be allowed to do those things in the first place.

To really fully understand how your data is collected, aggregated, shared, sold, and stored across the web of interlocking parties, you practically need a data science degree or at the very least have a really strong and solid contextual understanding of the data ecosystem. And it's unrealistic. It's unfair. It's inaccessible and frankly, unethical to ask everyone who uses the internet, which is a very broad range of people, to have that contextual understanding and to consider the far-reaching and material consequences in a single consent screen when they're in the middle of trying to do something else.

So my initial recommendation to you is to restrict

how companies can collect, use, and profit from data, shifting the burden of responsibilities from consumers to companies. After all, the data we produce is an extension of our own humanity, and that humanity deserves protection by our CPRA legislation. Thank you.

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

Our next commenter is Marshini Chetty. Marshini Chetty, please raise your hand. Thank you. Marshini Chetty?

Okay. We'll move on to Dona Fraser. Thank you. Okay. Ms. Fraser, you have seven minutes to speak. Your time starts now. You may use your camera if you wish. You may --

**MS. FRASER:** Thank you. Thank you. Good morning. So my name is Dona Fraser and I am senior vice-president of privacy initiatives at BBB National Programs. We appreciate the opportunity to address the California Privacy Protection Agency today regarding your upcoming rulemaking.

I'm proud to be here to represent our nonprofit organization headquartered near Washington, D.C. Our privacy team has more than twenty years of experience advancing privacy best practices and operating independent third-party accountability programs to help businesses and consumers navigate privacy challenges in

the digital marketplace. BBB National Programs works with individual companies, industry groups, and regulators to develop, monitor, and enforce robust privacy standards that have been built either on self-regulatory principles or legal requirements across various data types such as children's data, interest-based advertising, or cross water data transfers.

A key component of our mission at BBB National Programs is to bring stakeholders together in a self-regulatory environment to help craft enforceable and fair mechanisms that protect consumers in the marketplace and enable responsible businesses to compete on trust and accountability. In the area of dark patterns, more enforcement and accountability within the business community is needed.

Our view is that companies must be held accountable, not only to legal requirements, but also to industry best practices and standards. The prevalence of manipulative or deceptive design in the digital marketplace has led to legislative proposals such as California's current privacy laws to prevent consumer deception and preserve consumer autonomy. While the FTC acts prohibition on deceptive practices necessarily makes certain types of dark patterns illegal, it is far from a comprehensive, enforceable standard in the industry.

So through our work, we have come to know well the blurry edges that exist between poor disclosures and deceptive designs as well as the mismatch that often occurs when considering consumer experience and consumer privacy. We can say with confidence that a third-party, self-regulatory accountability program to establish standards in this space and monitor the marketplace for compliance of those standards would be a critical support to the work of this agency and the work of the FTC.

Regarding the specific term of dark patterns, I know from previous speakers today and in the past that we at BBB National Programs are not alone in strongly suggesting that laws, regulations, and the industry as a whole move away from using the term. The definitions under both CCPA and CPRA use the word design or designed, which more accurately pinpoints the behavior and practices the law desires to address.

Manipulative designs or deceptive designs would be more precise. And although the law does not determine intent, there is something quite implicit in the use of words such as manipulative or deceptive. For example, our Children's Advertising Review Unit, which was established in 1974 to protect children and their data in an online environment, monitors the marketplace for compliance with our self-regulatory advertising

guidelines which state that advertisement, apps, or games should not use unfair, deceptive, or other manipulative tactics, including but not limited to deceptive door openers or social pressure or validation to encourage ad viewing or in-app or in-game purchases or to cause children to inadvertently or unknowingly engage with an ad. And the guidelines go on to state that any method provided to dismiss or exempt must be clear and conspicuous. These same principles apply to the collection of data and avoid using the term dark patterns, instead describing the companies behavior and practices.

In addition to our recommendation on clear language around dark patterns and new rulemaking, we also recommend the following. And first is uniformity of disclosures. A required uniformity on the presentation of disclosures would likely reduce the use of deceptive or manipulative design. Such uniformity would prevent the use of language that may dissuade a user from making a well-informed decision. In our written submission we provided some examples to demonstrate the current range of disclosure language used across the marketplace.

Secondly, with regards to education. The California law, as we know, is aligned with the federal Children's Online Privacy Protection Act when dealing with data from

users under age thirteen. But for users age thirteen to sixteen, California requires an affirmative opt in to not sell personal information to a third party. This approach makes sense to us at BBB National Programs because we are deeply rooted in our understanding of the unique privacy risks for teen users who are not protected by COPA. However, additional education is required for businesses and consumers to ensure they fully understand the unique risks to the teen audience, particularly for those companies whose products are intended for users above thirteen years old and whom to date have not been required to implement age gates or other guardrails to determine whether their users are teenagers.

Should the agency desire additional information, we'd be happy to share a catalog of known risks that are unique to teen users.

Thirdly, efficacy of consent. At this point, we would ask is it enough to only provide consumers the ability to opt-out, or should consumers of all ages be able to easily and readily know whether their choices have been honored. And what is the recourse if their choices have not been honored, can efficacy be properly monitored and enforced? Then with that understanding, you could clearly define consent in the accountability mechanisms in place when user privacy is breached.

At BBB National Programs companies across various industries have proven their ability to hold themselves accountable to industry standards and best practices that align to stay in federal law when educated, informed, and held accountable. In such cases, government agencies, such as the FTC, act as a regulatory backstock when companies do not adhere to establish guidelines. In one such case, internet and social media advertisements made by Quicken Loans were referred to the FTC when the company failed to respond to an accountability inquiry by the national advertisement deficient of BBB National Programs.

In its advertising, Quicken Loans encourages consumers to refinance their mortgage --

**MS. HURTADO:** Thirty second warning.

**MS. FRASER:** -- about its low refinancing rates claiming no registration, no login. Further, the Quicken Loans privacy policy indicates it collects and shares personal data contrary to the implied message of the no registration, no log in claim.

The FTC supports independent industry self-regulation and keeps a transparent record of its actions in response to cases. This system requires that companies are held accountable not only to legal requirements, but also to industry best practices and

standards. If legal requirements are established that are clearly defined --

**MS. HURTADO:** Time is up. Ms. Fraser, your time is up.

**MS. FRASER:** Thank you. Thank you.

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

Our next commenter is Eric Goldman. Thank you. Okay. Mr. Goldman, you have seven minutes to speak. Your time starts now. Feel free to use your camera if you wish.

**MR. GOLDMAN:** Yeah. Hi. I'm Eric Goldman. A law professor at Santa Clara University School of Law where I direct the school's privacy law certificate. I blog post about the CCPA have all featured the dumpster fire GIF. I'm still deciding what GIF I'm going to use with my CPRA post.

I'd like to start by thanking the agency, board members, and staff for their hard work on this overwhelming project that voters assigned to it. It's a thankless effort that will garner criticism on all sides, so I'm grateful for your willingness to serve.

My first substantive point relates to the bills from the California legislature proposing to add new duties to the CPPA's remit. I'm baffled by these proposals because the CPPA's plate is already very clearly full. The CPPA

can -- already cannot meet the deliverable schedule approved by the voters so it's in no position to take on additional projects that would further compromise the CPPA's ability to meet its voter-approved obligations.

The CPPA's workload won't get any better after the CPPA completes its initial batch of rulemaking. The CPPA will then have the enormous and complex challenge that building an enforcement function from scratch.

Even more bizarrely, some of the legislative proposals have proposed adding nonprivacy matters to the CPPA's remit, such as making the CPPA responsible for children's well-being under the guise of defining dark patterns. This scope expansion is impossible because the CPRA's directives to the CPPA are privacy specific. So the CPPA lacks the ability to oversee nonprivacy topics while still adhering to its voter-mandated directives.

This takes me to my first suggestion. I encourage the CPPA to proactively and emphatically tell the legislature that, one, it cannot take on new privacy matters until its able to satisfy its existing voter directives; and two, it will never be in a position to take on non-privacy matters without completely restructuring the CPRA's directive to the CPPA.

My second substantive point is to observe how much of the CPPA's rulemaking, including most of the topics

covered by the stakeholder sessions, are essentially addressing empirical questions that we frequently have minimal or no empir -- independent and empirical research to answer those questions. As just one example, businesses apparently have been required to honor the global privacy control since AG Becerra tweeted about it in January 2 -- 2021, how's that going? Are there independent empirical studies of the GPC's costs and benefits since then? Is the GPC achieving its purported goals for consumers or not? The CPPA may not know the answers to those questions but the empirical answers are essential to the efficacy and legitimacy of any further CPPA rulemaking on the topic.

The same is true for any rulemaking on dark patterns. The CPPA has received a bit of empirical data on the topic but every detail of any dark patterns rule would be predicated on empirically answerable questions even if the CPPA doesn't actually rely on empirics when defining those details. In particular, there's been far too little independent empirical research into the CPPA's efficacy despite the fact that the CPPA has generated substantial field data over the past two years.

Worse, due to its timing, the CPRA did not incorporate any empirical findings from the CPPA -- I'm sorry, from the CCPA's operation. Given where we are

now, it would be very unfortunate to ignore these empirics in the CPRA's rulemaking without learning how -- from how businesses and consumers are actually behaving in the field, the CPPA could easily misdirect its efforts or possibly making things worse for everyone.

That takes me to my second suggestion. I encourage the C -- the CPPA to make explicit any empirical assumptions its basing its rules on, then when the CPPA does not currently have data in hand to support the assumptions it's making, the CPPA should, one, solicit independent researchers to study those empirical questions, and two, set sunset dates for those rules to enforce that they will be evaluated as new empirical data informs the questions.

The CPPA has enormous amount of hard work ahead of it. And again, I say thank you to those of you doing that work.

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

Our next commenter will be Jennifer Huddleston. Thank you. Okay. Ms. Huddleston, you have seven minutes. Your seven minutes starts now.

**MS. HUDDLESTON:** Thank you. Thank you for this opportunity to participate in today's stakeholder session. My name is Jennifer Huddleston and I'm a policy

counsel with NetChoice, a trade association dedicated to preserving free enterprise and free expression online.

As a CCPA -- I'm sorry. As the CPPA considers how to handle privacy rulemaking, the agency should avoid overly expansive actions that would penalize the uses of neutral technology in a way that may undermine many of the beneficial uses of technologies such as algorithms that consumers experience regularly. And can -- and these same technologies can even provide new solutions related to privacy, security, and authentication.

The CPPA should carefully consider the impact that its decisions may have beyond privacy and how they interact with existing laws and tools to resolve the underlying consumer concerns that the agency seeks to address related to privacy and security. As with any regulations, the agency should consider the impact these rules have on these technologies and users and ensure that the rules are grounded in their mandate related to privacy, and balance concerns about other issues such as speech and innovation.

The agency should avoid dictating a specific design that does not take into account the differences in technologies, types of data collected, and user preferences. And the agency should also consider how existing laws and regulations may address some of the

underlying concerns that it is seeking to address.

When it comes to dark patterns, the agency should be cautious of the negative impacts that overregulation may have and seek to address specific harms. Any regulations the agency considers should have clear definitions of the harmful behavior it seeks to redress to avoid unintentionally prohibiting neutral or beneficial practices and consumer privacy preferences.

As research around dark patterns has previously discussed, many of the concerns around manipulative options that are commonly referred to as dark patterns are most likely already capable of being addressed by existing precedents around unfair and deceptive practices.

An overzealous approach could result in an agency dictating user interface designs without full consideration of the distinctions in products, services, audience, or communication methods. In some cases, providing a very specific and clear feature, like a single button, may work simply. In other cases, a product may need multiple steps or multiple choices and a way to clearly communicate to a consumer what each of those different privacy choices may do to the user experience.

There might not be malicious intent, but rather an

attempt to ensure that consumers fully understand the impact of their choice on their experience with a -- with a product, service, or device. And we have a wide range of consumer preferences when it comes to their privacy online and the tradeoffs that they may be willing to make.

As with many privacy scenarios, often there are two great tools available to policymakers beyond regulation. And that is considering consumer education and redressing the harmful conduct through exist -- through policies that may already be in existence. This includes pursuing those bad actors who are engaged in deceptive and manipulative practices similar to as would be done in offline settings with regards to consumer protection violations, and that this enforcement be tied to specific consumer harms, as the laws were intended to. This can include providing clarity around the -- the harm seeking to be redressed, but it should also recognize that design differences may arise depending on the product and service being offered.

Policymakers should be cautious in perform -- in presuming that data collection or interaction with consumers is inherently harmful and instead seek to address only those specific actions that are harmful to consumers such as unfair and deceptive practices. In

addition to regulation, the agency should also consider less interventionist approach that would empower innovators and consumers to make choices that support privacy decisions that align with a consumer's individual preference and help the consumer identify when they may -- when they may notice a deceptive and unfair practice and what to do in those cases.

I thank you for this opportunity to speak during this pre-rulemaking phase, and I thank you for your time.

**MS. HURTADO:** Thank you for your comment, Ms. Huddleston.

Our next commenter will be Noreen Whysel. Thank you. Okay, Ms. Whysel. You have seven minutes to speak. You may use your camera if you wish. Your time starts now.

**MS. WHYSEL:** Good morning. I'm Noreen Whysel, director of validation research at the Me2B Alliance. I should note that today we've changed our name to the Internet Safety Labs. We are a nonprofit safety testing organization for connected technology, where I lead qualitative research to understand people's experiences and relationships with the technologies they use.

I'm a professor in communication design and CUNY's New York City College of Technology and have written and presented on research on dark patterns, accessibility,

and vulnerable populations. I would like to present our recommendations regarding CPRA and dark patterns and then describe them further during this time.

So first as others mentioned, stop using the term dark patterns. Focus on the harmful outcomes of these interfaces by calling them what they are: harmful UI patterns. Two, opt out should be the default condition, not a choice. This is a big one for us. Three, adopt a framework for identifying harmful UI patterns at each stage of the technology relationship. We also have specific recommendations about the definitions of consent and intentional interaction which I'll describe if I have time.

First of all, dark patterns. In CPRA, the definition of dark pattern affirms the designers are responsible for the effects of the UI pattern that causes harms. The outcome of the interaction is important. We stay in our B2B rules of engagement that technology should not willfully harm their users. But there is a willful neglect in adopting UI patterns just because they are easy, because they are embedded in the systems we use to design a product.

That said, I'd like to use my time to focus on the outcome of these harmful UI patterns, and notice that I didn't say dark. Industry is redefining so-called dark

patterns as deceptive patterns, and California should follow suit. Last month, Harry Brignull, the British ethicist well-known to have coined the dark patterns phrase, changed his dark patterns, dot, org website name and URL to deceptive, dot, design, following a trend championed by organizations such as the Web Foundation's Tech Policy Design Lab, who represent a new label as more inclusive.

In fact, we at -- we at the Me2B Alliance prefer the term harmful UI patterns, as it describes the outcome of the design pattern that affects the individual agency of the technology consumer. We know from our research that people understand they are being treated unfairly and they know that good UI patterns use clear and specific language so that they can make decisions without feeling coerced.

Two, opt out versus opt in. The alliance on opt out from data sharing as a choice requires a user action to be effected. This opens the door to harmful UI patterns. We support the practice of easy-to-use opt-in methods with opt-out set as the default. Requiring people to opt out is one of the harmful UI patterns frequently cited in literature in Brignull's research and is further defined in a dark pattern taxonomy developed by Purdue University's user experience, Pedagogy and Practice Lab

as the use of check boxes to opt out rather than to opt in. And this is listed and categorized in their taxonomy as interface interference.

Requiring opt-out whether paired with confusing wordings or not creates a isometrical power dynamic leading to harmful levels of data sharing and surveillance tracking and to a disruption of agency in people who use technology, and it does not promote the safety and wellbeing of people and is not harmonized with goalable norms. In addition, we should not assume people know they need to opt out. Instead allow people the agency to decide whether to opt in.

Third, a framework for identifying harmful UI patterns would be helpful, especially give -- excuse me -- especially given that many potential harmful UI patterns have yet to be designed. It would help designer to understand when they occur and what kinds of harms they cause. Harmful UI patterns exist along the spectrum of the entire technology relationship beginning before an account is made and/or other user relationship is established and until well after it is terminated.

I emphasize this because people don't always know that these UI patterns can exist before the traditional onboarding stages and after account termination. To provide clarity, the Me2B Alliance has identified what we

call a Me2B relationship life cycle or transactional stages that occur during technology use over time where consent to various actions occur.

These commitments map to the stages of social interactions as defined by George Levinger from acquaintance, buildup, marriage, deterioration, and termination. In each of these stages, there is a potential for introducing harmful UI patterns and negative UX outcomes.

In the initial acquaintance stage, for example, harmful patterns might include making it difficult to view content without creating an account, requiring people to share personal contacts, or enter a credit card number. In the buildup and onboarding stage, requiring access to contents or location information while signing up for newsletters, notifications, or loyalty programs when any of these data aren't -- aren't necessary or legitimate are examples of harms.

Long, convoluted, and nagging processes for closing an account or reducing other levels of commitments are also harmful. And requiring an opt-out or requiring people to deselect opt-in at any stage is harmful.

The establishment of each commitment may not be obvious to users, but in what we call the invisible parallel data universe, data is collected and shared with

third parties and a temptation to use deceptive or harmful UI patterns to accelerate data collection at each commitment stage is a risk.

These patterns are frustrating and can encourage people to stop using the service without closing their account which then preserves data sharing settings in perpetuity, another example of the unequal power dynamic between technology and user.

I've also had a couple of comments on the definition of consent and intentional interaction in the legislation. Because they use the term dark pattern in the case of consent which should be used -- or should be used as harmful --

**MS. HURTADO:** Thirty second warning.

**MS. WHYSEL:** -- in an intentional interaction, it sort of implies that opening a website is an intention to interact and we've all fallen for dark patterns -- for harmful patterns that are designed to get you to load something that you didn't intend to.

In sum, the regulations definition to -- of exactly what UX designs will constitute a harmful UI pattern remains unclear and requires specific guidelines, starting with language that aligns with global norms. Harmful patterns, not dark pattern --

**MS. HURTADO:** Excuse me, Ms. Whysel. Your time has

come to an end.

**MS. WHYSEL:** Thank you very much. I appreciate the opportunity to participate.

**MR. SOUBLET:** Thank you everyone for your comments on this session on dark patterns. We're now going to take a break until our next session on consumer rights to opt out, which begins at 12 o'clock when we will reconvene for that session.

Please feel free to leave the video on or teleconference open, or to log out now and back in at 12 o'clock when we begin that session on consumer rights to opt out. Thank you.

(Whereupon, a recess was held)

**MR. SOUBLET:** It's 12 o'clock. Good afternoon. I'd like to welcome you back to the California Privacy Protection Agency's May 2022 Pre-Rulemaking Stakeholder Session. I'd like to remind everyone that the session is being recorded.

Speakers that are scheduled for the current session on consumers' rights to opt out 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 are participating by phone, you will have already provided the number that you'll be calling from so that we may call you during your pre-

appointed speaking slot. Note your name and phone number may be visible to the public during the live session and our subsequent recording.

Speakers will be called in alphabetical order by last name during this window, and we will not be able to wait if you 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 screen.

Our moderator will then invite you to unmute yourself and also invite you to turn your camera on 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 short amount -- shorter length of time is just time. 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 remark, you're welcome to do so. You are also welcome to raise your hand during the public portion at the end of each day for general public comment.

Finally, you may also send us your comments via

physical mail or email them to regulations@CPPA.ca.gov by 6 p.m. tomorrow, May 6th. 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 the consumer rights to opt out session 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 consumer rights to opt out.

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

**MS. HURTADO:** Yes. Good afternoon. Our first speaker for this session is Robin Berjon. Robin Berjon, please raise your hand.

Okay. We'll move on to the next speaker, Justin Brookman. Justin Brookman, please raise your hand. Thank you. Okay. Mr. Brookman, you have seven minutes to speak. Your time begins now.

**MR. BROOKMAN:** Thank you very much. My name is Justin Brookman. I am head of technology policy at

Consumer Reports. Previously of the Federal Trade Commission and New York attorney general's office.

This is a session on the right to opt out, so I want to talk about the inherent difficulty of using opt out. If you generally don't want your data sold, then it is not practically possible to communicate that individually and separately to every business that you interact with. You have to scroll to the bottom of a website, find the link, engage with that opt-out process every site you go to, every store you go to you need to fill out a separate form, maybe for each transaction. Every app you have, you need to find the bespoke controls and individually opt out.

In general, people don't want to have to make granular privacy choices all the time. They don't want to deal with constant cookie consent screens asking them what kind of cookies they're fine with on any given website. They just want their services to work and for the vast majority of people, they universally do not want their data sold or shared to others.

So a year a half ago, Consumer Reports conducted an exhaustive study on the usability of CCPA opt-outs. We crowdsourced hundreds of people to the go to the California data Berger website and opt out of the sale of their data for just one data broker. As you might

expect, the results were pretty much a mess. Almost half of the sites people couldn't even find an opt-out link. People were asked for sensitive information, to upload a picture of their driver's license. They were told they needed to install -- allow cookies.

A lot of our survey participants just completely noped out of the process. They didn't finish even one opt-out. At least one person got added to a new marketing list trying to do a CCPA opt-out. And overall, half the people that we surveyed told us they were somewhat dissatisfied or very dissatisfied with the opt-out process. And that's just trying to opt out of one, one single company.

So for opt out of sharing to be usable in practice there need to be global opt-out options (indiscernible) broadcast to everyone all at once. They don't want their data sold or shared. This was included in CCPA and laid out in detail in the CCPA regs. This was added to the Colorado privacy law that was enacted last year. It was included in the Connecticut privacy law that was passed by the legislature last week. It was expanded upon in the CPRA.

So I will say I've been disappointed to see our lobbyists arguing that we should go backward. That honoring opt-out signals should now be optional under the

CPRA. That if a company receives a generally recognized symbol -- signal communicating that this person does not want their data sold or shared, then that company should feel free to ignore that under California law. Instead, companies should be -- consumers should be required to find and navigate hundreds or thousands of individual opt-out processes that are harder to use.

A lot of these processes actually predate the CCPA. They've always been around, but they've never actually been used. The reason the CCPA was passed in the first place was because these individual opt-outs were not practical or usable for folks.

And I will say this interpretation of optional opt-out -- optional response to universal signals is completely anathema to the spirit and the text of the CPRA. So under CPRA section 135, has two different options for a company to offer do-not-sell choices or do-not-share choices, depending whether the company reserves the right to -- to push back, or nudge the consumer. But section 135(e) is quite clear. A consumer may authorize another person to opt out of the sale or sharing of their data including through an opt out preference signal indicating the consumer's intent to opt out, and a business shall comply with an opt-out request received from a person authorized by the consumer to act

regardless of whether the business has elected to comply with subdivision A or B of the section. The text is clear. CPRA was intended to build upon and extend the CCPA, not to back track.

I will say that if CPRA is interpreted to counterintuitively not require adherence to universal signals, then in practice the law is going to be a failure. And consumers are not going to -- Californians are not going to have the ability to practically limit the selling or sharing of their data.

I do think there a few ways that CPPA can make compliance with universal signals easier for companies. I think the CPPA should host and update a list of signals that should be interpreted by folks as binding CPRA requests. You know, they could -- maybe different signals for different user agents, the webs browsers have some signals, mobile devices may have a separate signal for apps to respond to, smart TVs might develop their own global opt-out signal for different apps on the TV. It's still difficult, TV is, for consumers to manage settings on different devices, but it's still easier than per website, or per app, or per channel.

And I think it's completely reasonable to give companies some grace period when a new signal is adopted to give them some time to code and to be able to respond

to -- to those signals.

Finally, I just want to add that I am worried about companies responding to universal opt-out signals with constant requests to ignore it. This is why the CPRA actually adopted the bifurcated structure that it did. But I don't think absolving companies of the need to put up do not sell wings is going to be enough incentive for them to not bug the user and say hey, can we ignore this signal.

So I think the CPPA is going to need to put up guard rails on when and how companies can ask to ignore signals to -- to guard against abusive dark patterns, and to not recreate the European experience of just relentless, countless, confusing consent screens that consumers don't want. They just generally want it to work. And for -- again, for most people they just don't want their data sold or shared.

Thank you very much for your time. Happy to answer any questions folks might have.

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

Our next commenter, we are going to try Robin Berjon again. Thank you. Robin Berjon, please raise your hand.

**MR. BERJON:** Hello. I believe it works now. Sorry about that.

**MS. HURTADO:** Okay. Thank you. Thank you very

much.

**MR. BERJON:** Zoom troubles. Thank you.

**MS. HURTADO:** Okay, your seven minutes will start now, Mr. Berjon.

**MR. BERJON:** Thank you very much. So hi everyone. Thank you for your time, and thank you for inviting me today. As just mentioned, my name is Robin Berjon. I am VP of data governance at the New York Times, and my focus there is on privacy but more broadly on sustainable business models around data for news publishers. The feedback that I'm offering today is based on my team's work implementing the CPPA's do not sell opt-out across all New York properties and also in supporting the global privacy control or GPC signal in production on NYTimes.com for well over a year now.

The first thing that I want to say is -- is from a strictly business perspective. The more people opt out, the better for us. Broadcasting personal data might help with next quarter's bottom line and that's actually why -- why people do it, but longer term, as a publisher giving away our audience data for third parties to profit from independently is equivalent to tossing your -- you know, our most valuable asset out the window.

People think of opt-outs as a privacy issue and it really is, but just as importantly for us it is an

opportunity to reach out business practices that are not detrimental to publishers in the way that today's inconsequential data practices are. We don't typically share precise audience numbers, but the quite significant numbers of Californian readers have opted out on our properties and we find that excellent. The (indiscernible) opt-out state represents for us, you know, some kind of really pragmatic compromise in which it's possible for us to -- to show effective and relevant ad campaigns but without giving away our core data assets to third parties.

And so you know, one thing I really want to emphasize here is that the ability to rely on a -- you know, as part of this opt-out structure on a standardized signal like GPC for us is -- is a really big win. It makes it significantly easier for people to opt out, which in turn is good for us as publishers. Implementing a standard signal like GPC is a lot simpler and a lot cheaper and it also makes delivering ads more efficient, which in turn just makes us money. And also, you know, I think it would be confusing to people if some sites support GPC and others had do not sell buttons, so I really think that from a -- from a pure user experience and a pure coherence perspective, both are needed.

But you know, returning to GPC. Supporting GPC

makes things really simpler for people and businesses, and I've been a bit disappointed to hear GPC being described as complex because GPC is just one bit of information so that's just basically the smallest amount of information possible. And I think that -- you know, I really wonder if a company that finds manipulating one bit daunting is really equipped to -- to properly handle any amount of personal data.

One thing that -- that is also relevant I feel as someone who works in standards and has been working around browsers for the past twenty years, it's the question of whether browsers and other such systems would be able to set the global privacy control and the GPC signal on by default. And I think that if they didn't, we might wish to look at it as potentially as a deceptive claim when they -- when they make privacy claims. People overwhelming expect their browsers not to share data with third parties. GPC is evidently an improvement to privacy and it's really easy to -- for browsers to implement. Several have already done it.

So I feel like it would be deceptive for a browser to claim that they care about their user's privacy but not have GPC on by default. So you know, with this in mind, I really think that having GPC on by default in browsers is the only option that realistically matches

people's expectations.

On a small negative note, and this is the -- pretty much the only negative note that I have to report from the do not sell experience. The CCPA added regulations added a requirement that -- that I feel was a mistake. The initial, you know, do not sell button experience that the Times had implemented was such that the user would just click it and immediately be opted out.

Instead the regs made it a requirement for us to show a notice after the user had clicked the button, and this just degraded the experience. We really feel that exercising one's rights should be a pleasant experience and so if at all possible, please do -- you know, let -- do not make us ruin the opt-out experience with additional notices.

But apart from this small issue, I really want to return, you know, to emphasize that our experience of running do not sell has been positive. It's been positive from a business standpoint. The availability of a standard GPC signal is great for us and for our readers, and I really hope that this is the first step towards a future in which the digital business models that we have to rely on are better for both privacy and publishers because these two things are very much aligned. With this, thank you so much for your time and

I wish you an excellent day.

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

Our next commenter will be Ronak Daylami. Ronak Daylami.

**MS. DAYLAMI:** Hi.

**MS. HURTADO:** Hello. You have seven minutes. Your times starts now. Thank you.

**MS. DAYLAMI:** Thank you. Good afternoon. My name is Ronak Daylami. I am the policy advocate on privacy and cybersecurity issues for the California Chamber of Commerce speaking today on behalf of our 14,000 members who employ over 25 percent of the private sector workforce in California. My personal experience in this area also includes staffing the authors of the CCPA throughout the passage of that law in my formal role as the chief consultant for the assembly privacy committee.

I cannot stress enough that businesses both want to comply with the law and support privacy rights and regulations that are clear and workable. This is the perspective from which we approach these topics, trying to identify operational issues and intended consequences to make compliance both feasible and less burdensome on businesses and to ensure that the rights operate as intended in practice.

We thank you for providing us the opportunity to

speak here today. Our primary feedback will be on the issue of the global opt-out signal.

First and foremost, we want to stress that the global opt-out preference signal is voluntary under the CPRA as approved by voters in 2020. The CPRA does not actually mandate businesses to provide a global opt-out signal. It provides businesses the option and requires regulations around that voluntary use.

Subdivisions A and B of section 1798.135 of the civil code gives businesses three options. A business can have one do not sell or share my personal information link as well as a separate limit the use of my sensitive personal information link, or they can have a single link that does both. Alternatively, the third option is to not have any links as long as they recognize an opt-out preference signal. This allows businesses the opportunity to implement the most effective method for their particular situation while still providing individuals the opportunity to opt out of the use of their PI.

Second, we strongly believe that regulations that address the requirements of this voluntary signal must be developed with industry input to prevent unworkable standards and to prevent anti-competitive impacts. We have concerns over the possibility that consumer send --

over the possibility of consumers sending conflicting signals, which would create significant compliance burdens for businesses. The risk includes a scenario where a consumer uses a universal opt-out but then opts in for a specific service. We request explicit guidance around such scenarios.

Additionally, while the CPRA contains numerous helpful guidelines for issuing technical specifications for any opt-out preference signals, it's unclear to us how businesses will know which signals meet the requirements that this agency comes up with. Third, we strongly stress the need for harmonization. Consistency across state lines is critical as more and more states are issuing similar laws and regulations to adopt their own opt-out signal requirements. Harmonization helps ensure compliance.

We suggest specifically looking at the states of Colorado and Connecticut. Similar to CPRA, Colorado requires clear communication of a consumer's affirmative, freely-given, and unambiguous choice to opt out. Colorado also, however, prohibits the rules from adopting a mechanism that is a default setting, and it requires that the signal also permit the controller to accurately authenticate the consumer as a resident of the state and determine that the mechanism represents a legitimate

request to opt out. We believe such elements should be considered here as well.

Our fourth point revolves around how businesses process opt-out signals. As a technical matter, a business may not be able to recognize a user from a browser signal. Signals should only apply to recognize identifiable consumers in order to avoid the risk of a choice only being recognized on an individual browser. Technical standards should also ensure that the signal accurately identifies the residency of the user so the business knows that the user is exercising an opt-out choice under CPRA.

However, businesses should not be required to identify unauthenticated users to ensure that they are opt out of all forms of selling or sharing PI. The CPRA specifically states under subdivision J of 1798.145 that the act shall not require reidentifying or otherwise linking information that in the ordinary course of business is not maintained in a manner that would be considered PI.

Fifth, a global signal should also permit consumers to reverse their decision and opt back in if they so choose, both as a general matter and for specific use cases for specific businesses as well. As such, we need further clarity on how businesses can provide consumers

who have previously indicated they wish to opt out via the signal with the opportunity to consent to the sale and sharing of the PI or the use and disclosure of their sensitive PI with that business specifically. The regulations could allow businesses to use a pop-up window or other form of consent for this purpose.

Sixth, opt-out signals must -- excuse me -- must not come with default settings and businesses must have the right to notify consumers of the benefits and consequences of opting out and the use of cookies. This promotes informed choices and gives effect to the statutory requirement that the signal be sent with the consumer's consent, where consent means any freely given, specific, informed, and unambiguous indication of the consumer's wishes.

A couple other points I'd like to make in my remaining time. On the right to correct -- accurate information is in the best interest of both consumers and businesses. Companies already have existing ways to allow consumers to correct their data and shouldn't have to build new systems just for CPRA. We urge the agency to allow flexibility in how right this is effectuated. Similar for example to how existing regulations on CCPA's right to delete allow for flexibility when data is in backup systems.

The right should be limited to correcting only that PI which is necessary for the consumer to receive services and exercise rights related to the business such as their name, contact information, payment information. It should not extend to data points such as the consumer's IP address.

Regulations should also consider situations where that effort to correct may be disproportionate to the benefit to the consumer. To state it another way, efforts by businesses should be commensurate with the significance of the data's impact on the consumer. If for example data is no longer being used for commercial purpose and is archived based on legal requirements, that would require significant effort to correct.

Next, we strongly believe that regulations for -- regulations for automated decision making ought to be limited to fully automated processes that make, not just assist, final decisions without human intervention and that have legal or similar significant effects on consumers, such as in the realm of housing, lending, medical benefits, and so forth as articulated in other state laws such as Colorado.

This avoids capturing everyday low risk automated technologies that enable businesses to serve consumers at scale such as spreadsheets for computing software.

Furthermore, we caution that any broad right to -- broad right to opt out of ADM is not supported in the text of the law and could undermine an otherwise helpful process to both companies and consumers.

Lastly, on cybersecurity audits and risk assessments, any audit requirements should only apply to those systems that engage in high risk processing.

**MS. HURTADO:** Thirty second warning.

**MS. DAYLAMI:** Reporting obligations to the agencies should be clarified to reveal -- to avoid revealing security or other vulnerabilities that could result in additional risk to proprietary information disclosed. We also ask that the agency recognize well accepted standards for cybersecurity audits, such as ISO and NIST, and allow for information security policies that align with similar industry standard frameworks.

With that, thank you for your time.

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

Our next speaker will be Dan Frechtling. Okay. Okay. Mr. Frechtling, you have seven minutes. Your seven minutes starts now. You may use your camera if you wish. You're muted.

**MR. FRECKLING:** Thank you. Hi there. I'm Dan Frechtling, CEO of Boltive. We're a software company doing business in California that exposes personal data

leakage. I wish to speak on the ways current technologies and methods used today routinely interfere with consumer rights to opt out.

As important as it is to address dark patterns, it's just as important to address dark signals. And dark signals are consumer opt-outs that fade as they're passed to downstream parties in cross-context behavioral advertising. Consumer choose to opt out or opt in, but with dark signals this choice is never received by those that are buying ads. Dark signals endanger consumer opt-out rights.

Dark signals occur in real-time bidding, the process that powers cross-context behavioral advertising. It's an auction is 200 milliseconds and it -- it plays a worthy role, like delivering relevant messages to consumers, but there are vulnerabilities.

Here's an illustration that starts with a mobile website here, and for opt-outs to work with real-time bidding, the website needs to communicate with the supply side platform, the exchanges and networks, demand side platforms, all the way down to where the advertiser is. And this can involve fifty or more vendors per website. Leaks can happen anywhere at any interface between these parties. And these third parties make code changes periodically which can cause data leakage.

Critics of real-time bidding say that it passes personal information about geolocation, health, religion, sexual preference, and ethnicity. Because CPRA came about partly to restrain excesses in cross-context behavioral advertising, Boltive recently completed a study to see how many of the Fortune 100 use opt-out technologies that are both compliant with the law and work with web protocols like real-time bidding.

Boltive's auditing tool creates secret shoppers to expose exactly where the leakage is we found two-thirds of the Fortune 100 used consumer opt-out methods that are either legally unapproved or cause dark signals.

We classified five methods of opting out of data sharing, and our intention here is to inform, not endorse. The first is industry consortia, which are used by sixty-nine firms in the Fortune 100; web forms that are used by forty-seven firms; consent management platforms, forty-two firms; offline methods, eleven firms; and user-enabled methods like GPC that none of the firms appeared to be accepting.

Firms are required of course under CCPA to use two or more methods. And what we found where they succeed or fail, the industry consortia model such as the Digital Advertising Alliance, the Network Advertising Initiative, or the 127 vendors participating, is the most popular.

The underlying technology works with those -- those partners 98 percent of the time, but the consortia appear to be in question by two OAG published notices of alleged noncompliance last year.

Online web forms are second most common. They have precedents since consumers use them to opt out of email communications. They are permitted by CCPA in section 135(a), but they too don't integrate well with real-time bidding when not logged in, which is very rare. Further, Boltive has found that 62 percent of the forms don't delete, some are all third-party browser cookies, so personal information is still shared down the chain of vendors.

Consent management platforms are the third most common. They are allowed by CCPA. But Boltive software finds these handshakes fail 25 percent of the time in real-time bidding.

And offline methods such as phone and email are the fourth most common. They're specifically mentioned in 11CCR999.315(a), but they're incompatible with real-time bidding.

And lastly, user-enabled methods, also called global opt-out preference signals, like the GPC and the ADPC, they are efficient as Justin Brookman and Robin Berjon pointed out, but none of the Fortune 100 have adopted

them based on our research.

So our research shows two-thirds of the Fortune 100 are not effectively handling consent and dark signals endanger consumer opt-outs. In one example, Boltive found a foreign company known for ad fraud extracting data to build profiles of consumers. In a recent example, we found advertising to manipulate public perception of the Russian invasion of Ukraine.

But most of the time, data leakage is unintentional. Usually, companies are acting in good faith. They and their vendors, though, use opt-outs methods that don't work. And we need rules to ensure opt-outs methods are both legal and effective.

To address this, CPPA rulemaking must ensure that dark signals do not endanger consumer opt-out rights in cross-context behavioral advertising. Clearly, the intent of CPRA goes beyond advertisers and data controllers to downstream partners and data processors, but statute's not clear in this regard.

The CPPA can clarify requirements and technical specifications for an opt-out preference signal and section 185(a)(19)(A) must include accurate transmission of opt-outs to all third parties and cross-context behavioral advertising. Companies should then be audited for transmission of opt-outs and action taken by parties

in the advertising chain. Only then can consumers feel safe their opt-outs are not misinterpreted as opt-ins.

Without this supervision, dark signals endanger consumer opt-out rights. The rules today are like delivering goods when a stranger presents a payment method but not checking to see if the payment actually went through. Furthermore, the CPPA can ensure the audit authority mentioned in section 185(a)(18) includes verifying that opt-outs are authentically passed and received by parties in the advertising chain.

Now monitoring the multitude of opt-outs by consumers may seem a tall task. Fortunately the businesses or CPPA can use privacy enhancing software that requires no installation. With cloud software, you can orchestrate 100 percent compatibility, something that both online firms and regulators may find of interest.

So in closing, if rules don't require opt-out signals to function down the chain, companies may do just enough to meet the letter of the rules, leaving consumers exposed. But if CPPA rulemaking mandates that consumer choices accurately flow through vendors, similar to checking that the payment actually goes there --

**MS. HURTADO:** Thirty second warning.

**MR. FRECHTLING:** -- CPRA can through this ensure dark signals do not endanger consumer opt-out rights.

Thank you for this opportunity.

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

Our next commenter is going to be Margaret Gladstein. And Margaret Gladstein will be joining us via phone. Okay. Ms. Gladstein, you've been unmuted. Your time starts now. You have seven minutes.

**MS. GLADSTEIN:** Thank you. My name is Margaret Gladstein, and I'm here on behalf of the California Retailers Association.

CRA is the only statewide trade association representing all segments of the retail industry, including general merchandise, department stores, online markets, restaurants, convenience and grocery stores, chain, drug, and specialty retailer.

Retailers have a unique role in the privacy discussion because our interests are closely aligned with the interests of our customers. Our members interact with our customers every day. Fortunately we're now back to serving more people in person. If we aren't giving them what they want, from goods and services to privacy protections, they will tell us by making different choices about where they shop and what data they share or whether they share data at all.

California retailers believe the regulations should

respect and empower California consumers by making sure retailers are allowed to honor their specific choices. Civil code section 1798.135 is clear. Honoring a universal opt-out signal is optional. We encourage you to adopt legislation that does not frustrate consumer choice and recognize that when consumers have specifically made a choice, that specific choice should outweigh a general opt-out browser setting.

That said, because there are -- there are certainty -- excuse me. That said, there is uncertainty right now with the opt-out signal because there are no guiding principles regarding its creation, implementation, universality, and the ability to ignore it when appropriate. A universal opt-out signal should not be left to the devices of any single organization to create, especially an organization that operates outside the purview of this agency.

The signal should be created with the required input from industry so that no one entity exerts outside influence on the signal standards. This would make sure California consumers have the benefit of a regulatory systems that is clearly transparent and functional for them. It would keep the number of signals to a minimum, ideally just one, so there would be no conflicts among signals.

The signal needs to apply to only recognized customers and be applicable across browsers and devices. It should also make sure consumers retain the right to opt-out, to opt-in, or to reverse any opt-out selection. Without these requirements, the system risks confounding and frustrating consumer expectations and running counter to their desires as multiple entities create differing signals.

If this happens, California businesses, especially small businesses, will experience significant compliance costs. We encourage the agency to outline a clear path for consumers who previously opted out and then choose for themselves to opt in for specific business or use cases.

I'd also like to briefly discuss the CPRA definition of dark patterns. CRA believes that this definition runs the risk of being overinclusive because any user interface that structures a user experience could be interpreted as having an effect if limiting user choice to the options that are provided. Designers have to make choices in creating user experiences. Attempting to design an interface that provides a user with control where every theoretical choice could exist would not serve consumers and would be impractical. The agency can provide clarity by specifying the position of dark

patterns as focused on design practices that amount to consumer fraud.

I would like to address one more area that can be particularly difficult for retailers if not properly dealt with by this agency. That is whether the processing of personal information in the context of employment should be covered by these regulations. We believe employment related information should be excluded.

The risk to individuals' privacy regarding collection and processing of personal information in the context of job applicants and employment, independent contractor relationships would not outweigh the benefit, where the personal information is collected and used solely within the context of an individual's role or former role as a job applicant, employee, or independent contractor. Any risk to the privacy of individuals in the HR context is far outweighed by the significant confusion such legislations would create for California workers and the substantial compliance burden they would place upon businesses of all sizes, especially small businesses.

Regulations about personal information or sensitive personal information would necessarily result in significant confusion and costs to conflict with the

litany of state and federal employment laws governing personal information in this area. HR data should be excluded from these regulations. But if they are included, they must, one, not impose an undue burden; two, permit an opt-out process resisting internal HR platforms and finality; and three, not conflict with the ability to comply with state and federal laws, civil, criminal, or regulatory inquiries, investigations, subpoenas, or summons, or to exercise or defend against legal claims.

The California Privacy Protection Agency has a great opportunity to create a strong privacy framework that works with consumers and businesses alike. The California Retailers Association appreciates the opportunity to make comment. And we encourage you to find balance by adopting reasonable regulation that meet consumers' privacy needs and expectations while still enabling retailers to offer the products and services consumers want. We look forward to providing our assistance and counsel in that process. Thank you.

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

Our next speaker will be Stuart Ingis. Stuart Ingis, please raise your hand.

We'll move on to Tom Kemp. Okay, Mr. Kemp, you may use your camera if you wish. You have seven minutes to

speak. Your time starts now.

**MR. KEMP:** Hi. Can you hear me?

**MS. HURTADO:** Yes, sir.

**MR. KEMP:** Okay. Great. So hi, I'm Tom Kemp. And I am a long-time software security executive. I've cofounded a couple companies and also been heavily involved in the privacy world. I specifically worked on the Prop 24 campaign. And most recently, I've proposed SB 105-9 to enhance the data broker registry law that moves the registration and regulation of data brokers over to the California Privacy Protection Agency.

So there's a couple of issues as it relates to the consumer's right to opt out that I wanted to discuss in my seven minutes.

The first issue is that consumers actually don't know their rights. And so there was a recent survey done by Consumer Action and the Consumer Federation of America that many consumers have actually not exercised their rights under the CCPA to see and delete their personal information collected about them and to request their information not be sold. And it turns out the top reason given for not exercising these rights was not knowing about them. So we just have a fundamental issue. If you want to get consumers on the topic of consumer's right to opt out, you need to have consumers know that they can

actually do that.

The next issue is that consumers are really facing a scavenger hunt when they do exercise their rights. And I know Justin with Consumer Reports talked about the survey that they did a year and a half ago and it was painful to read in that customers failed to locate the required links to stop the sale of their information. Some do not sell processes, involve multiple complicated steps to opt out. And over 50 percent of the time, the actual consumer was somewhat dissatisfied or very dissatisfied with the opt-out process.

So first of all, the first issue is people don't know they have this actual right. The second issue is, is that when they do know they have the right, that they struggle to actually be able to exercise this right.

The third issue is that it turns out that customers don't even know who has their data and so there's these entities called data brokers that collect consumers' personal information and resell or share that information with third parties. The key definition of data brokers is not only that they sell or share to third parties, but they have an indirect relationship. And so because companies -- these companies, data brokers, never interact with consumers, consumers are unaware of their existence. And -- and so the problem is, is that they

don’t know who to go to to be able to exercise the rights.

And what's frustrating is, is that Vermont first and then California implemented a law -- in the case of California, AB 12012 -- that mandates the registration of data brokers. Now take into account that there's 4,000 data brokers in the world. Many estimates from organizations like EFF and EPIC and the Privacy Rights Clearinghouse say that there are thousands. And when the law was passed, the attorney general said, hey, we expect 1,000 data brokers to actually register, which would give awareness and visibility to organizations and -- and consumers to know who they should contact to exercise their rights.

But the problems is, is that only 400 -- 10 percent -- of the worldwide data brokers, and 40 percent of the expected data brokers have actually registered. And the headlines are screaming with issues regarding phone location data, mental health apps are sucking information out and they're trading that. We have a priest was even outed because it tracked that person's location, et cetera. And just the other day, a reporter was able to purchase phone location data from a data broker for people coming and going from Planned Parenthoods and they only had to pay 160 dollars. So we

also as consumers lack visibility on who actually has our data as well.

So I have three specific proposals on this particular topic that I want to raise with the Privacy Protection Agency. Number one is that the Privacy Protection Agency should do public services announcements to educate consumers regarding their privacy rights. Prop 24 gave a 10 million dollars per year budget to the PPA. Because staffing is going slow and steady -- and I know Ashkan and the team are doing a good job. It just takes time, right.

I estimate that there's probably going to be an unused budget of this fiscal year of 7 million dollars. And given that enforcement doesn't kick in to mid-2023, there will probably be -- it just -- you can't hire the people and spend the money on doing regulations. There's probably going to be an unused budget of 5 million dollars next year. These are just my, you know, estimates off the top of my head right here, but it's going to be over 10 million dollars over the next two years. The PPA has the money and it should spend it on public awareness.

It specifically -- if you look at the requirements in Prop 24, there's -- a number of requirements of the PPA have to do with evangelism, specifically section

1798.99.40(e) says that the PPA shall provide guidance to consumers regarding the right under this title. So spend this unused money because the law says you guys should be providing guidance to consumers to address that --

**MS. HURTADO:** Thirty seconds.

**MR. KEMP:** -- (indiscernible). The second requirement is, is that there is a privacy interaction tool that can be enhanced that should be the call to action.

And the final thing is, I definitely urge that the PPA look at data brokers -- obviously you guys can't publicly support SB1059, but I do think that there needs to be more sunshine and transparency with companies that we don’t have a direct relationship that share and sell our data.

So thank you very much.

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

Our next speaker is going to be Justin Kloczko. Thank you, Mr. Kloczko. One moment. Okay. Mr. Kloczko, you have seven minutes. If you wish to use your camera, you may. Your time begins now. You're on mute.

**MR. KLOCZKO:** Sorry about that.

**MS. HURTADO:** Thank you.

**MR. KLOCZKO:** Hello everyone. I'm Justin Kloczko with Consumer Watchdog. And we are particularly

concerned about precise geolocation in cars and anticipate the board will draw strong rules to allow users to opt out of geolocation.

So car data is the new gold rush of the auto industry. This year nearly all of new cars on the road will be connected, meaning they will be essentially smart phones on wheels. Automakers and third-party companies know where we drive, what we buy, eat, our texts (audio interference) what time (audio interference). A whole consumer profile is created with this information to -- to essentially sell you things. The targeted advertising we see in our browsers, inboxes, and social media feeds is -- is coming for the driver's seat.

Currently, car infotainment systems, like Chevy's OnStar services, feed users data to apps like Domino's and Shell. This is according to a Washington Post investigation. Starbucks knows your geolocation so it could know the best time to divert you through a drive-through, and so this kind of amounts to what has been called "behavioral modification".

The software company, Telenav, is developing in-car advertising. It's touting a freemium model similar to streaming services like Hulu and Spotify, where in exchange for free services, drivers will be flashed with ads. It made a post on its website saying why in-car

advertising works. And in Telenav's case, it basically amounted to "advertising is worth it to the consumer while disregarding safety and privacy".

One of these companies that sources location data with car companies is Otonomo. The company itself has said collects 4.3 billion data points a day, and in an internal company presentation says that thousands of organizations have access to Otonomo's data, and just last week it was hit with a lawsuit in California over its geolocation tracking.

So simply put, cars don't need to know your geolocation to just drive. Manufacturers argue opting out of geolocation will take away emergency services for drivers in case of an accident. This is an argument presented by the Alliance for Automotive Safety (sic); it's a car lobby whose members include Ford, GM, Toyota, and virtually every automotive manufacturer. It sued the state of California over lowering vehicle emissions, it sued the EPA in order to lower ethanol and gasoline, and it recently has fought the right to repair law that voters have passed in Massachusetts. And in its proposed rules to the board, the alliance warned "if a consumer opts out of automated decision making that supports a car crash avoidance system, that system would no longer be allowed to help avoid or mitigate the impact of a crash".

So they are weaponizing safety and using the same tracking consent form for a host of other reasons, and it's a false choice. Consumers don't have to choose between their safety and having their data used for other tracking purposes.

This agency's rule should force manufacturers to unbundle consent for tracking for a paramedic from tracking for other reasons. And manufacturers are also urging the agency to not require them to provide access to personal info because in most cases, companies say they do not know who's driving a particular vehicle. But how do they not know that if they have customers' consent in the first place?

This commission has the power to require companies to stop the use of geolocation for anything other than what it is intended for. Companies simply don't want to do it. We expect the CPPA will introduce rules that require companies to limit their collection of geolocation for the intended use of safety location, not for any other use, such as marketing.

The danger of this type of surveillance is profound. Auto insurance companies will discriminate against people based on neighborhoods they frequent. Law enforcement agencies already have access to this data and evade traditional warrant requirements by tapping into

information uploaded from a USB port. Companies will also say they use anonymized data, when often that might not be true. Anonymized data when paired with other leaks or data points, such as credit card usage, can be used to identify you and target you according to technologists we've interviewed, and news reports.

A German study looked at anonymized user vehicle data, found that just fifteen minutes worth of data from brake pedal use could identify the right driver. And a Stanford and Princeton study showed that deanonymizing user's social networking data was pretty simple.

The CPRA currently defines precise geolocation as "any data that is derived from a device and that is used or intended to be used to locate a consumer within a geographic area that is equal to or less than the area of a circle with a radius of 1,850 feet". Car data falls under this definition. The CPRA also recognizes that precise geolocation is a type of sensitive personal information, thereby giving consumers the right to limit its use and disclosure in certain circumstances. (Audio interference).

Aside (audio interference) concerns, distracted driving is a big concern as the industry clearly wants to commodify its data and advertise to you. One of the biggest misconceptions is that technology is making

driving safer, and it just isn't. The past couple of years saw big increases in traffic fatalities, prompting the federal government to take action. And the death toll could grow if companies can increasingly turn our vehicles into vessels for consumerism.

And as many of you know, we live in an area in an era of surveillance capitalism --

**MS. HURTADO:** Thirty seconds.

**MR. KLOCZKO:** -- and that's why it's important that geolocation can be addressed. People should be able to opt-out of location data in cars just like we can with our smartphones. And so thank you for your time.

**MS. HURTADO:** Thank you so much for your comment. Our next speaker will be Keir Lamont. Keir Lamont, please raise your hand. Okay. Mr. Lamont, you have seven minutes. Your seven minutes starts now.

**MR. LAMONT:** Thank you for the opportunity to participate. My name is Keir Lamont, and I am counsel with the Future of Privacy Forum. FPF is a consumer privacy nonprofit that provides resources and independent analysis to policy makers based on our work with privacy professionals, advocates, and scholars.

I would like to direct my comments towards the consumer right to opt-out of the sale and sharing of personal information under the California Privacy Rights

Act, and specifically, the Act's delegation of rulemaking authority regarding opt-out preference signals under CPRA Section 21(a), paragraphs 19 and 20.

A data protection regime rooted primarily in individual controls and consent options is, as Mr. Brookman and Mr. Kemp described, overwhelming and unmanageable for ordinary people in practice. The development of user-selected universal opt-out mechanisms expressed through browser settings, plug-ins, or other technologies is intended to help solve this issue by automatically conveying individual requests to invoke privacy rights to all businesses that an individual interacts with, at least within a particular media.

For example, a browser plug-in is capable of sending signals to all websites that the browser visits, while a mobile device platform setting may be needed to send similar signals to apps. As a first order matter, comments from earlier speakers have shown that there were divergent views as to whether the plain language of the CPRA requires that businesses recognize qualifying opt-out preference signals. However, regardless of how this question of statutory interpretation is ultimately resolved, California has led the way on this issue by -- and also prompted additional states, notably Colorado and Connecticut, to include and unambiguously require the

recognition of opt-out signals in forthcoming privacy laws. By virtue of its rulemaking authority, the CPPA therefore has an important opportunity to contribute to the nationwide development of BedRock (ph.) technical and policy principles for preference signals.

I would like to highlight three major issues for the development and implementation of signal preferences. One, standards are needed for responding to different requests from different tools, browsers, devices, and business-specific privacy settings. Two, there are practical and policy questions for the association of an opt-out request with data collected from different sources. And three, there was a need to establish a forward-looking, multistakeholder, multijurisdictional process for recognizing qualifying preference signals under emerging U.S. state laws.

First, rulemaking should address what to do when a business encounters conflicting signals or signals that are inconsistent with other expressions of choice. Consumers today face an expanding labyrinth of signal choices across different platforms, technologies, and business-specific privacy settings. In this environment, there are many occasions where a business may receive signals that appear to be duplicative, differing, or in conflict with each other.

For example, most individuals will visit websites through multiple browsers and devices which may each send multiple or different opt-out signals that may be set in different configurations. Furthermore, some of those websites will display cookie banners asking for consent to sell device browsing history to ad networks. Meanwhile, other websites will have authenticated relationships with users and may offer individualized privacy controls and choices, like through a privacy dashboard.

In many cases, qualifying opt-out preference signals should override other settings; for example, when consent comes from a cookie banner, which does not provide real and meaningful choice. This is the approach taken by lawmakers in Connecticut, which in forthcoming Senate Bill 6 requires that businesses must respect global opt-out signals as overriding other business-specific privacy settings with, however, an opportunity to provide users with notice of the conflict to ensure that consumers prove preferences or respect it. However, in other cases, it may be appropriate to consider an individual's separate privacy settings set with a specific service or platform, or written consent offered in an offline context, which, it may be appropriate to take precedence.

Second, the agency should clarify the extent to

which opt-out preference signals can be expected to and should apply to separate sets of personal data. For example, an individual might have both an online and offline relationship or account with a retailer and may occasionally visit that retailer's website without logging in. When that happens, sending an opt-out signal would be directly associated only with information from that individual's browser encompassing an IP address, cookie IDs, and other header information. That data may or may not be readably linkable to the user's full identity or existing account with a retailer, or might only be linkable by taking additional identifying steps.

If an opt-out preference signal sent through a browser can be reasonably linked to a person's full identity, account, or other offline information, a secondary question arises as to whether the signal request should apply to that additional information. In some cases, extending the effect of the signal to other data sets could be inconsistent with what users expect in enabling a particular plug-in or other request mechanism. The answer to this question may depend in part on the disclosures that individuals receive when they select and enable a specific opt-out tool.

Finally, I would like to close by emphasizing the need to establish a forward-looking process for

designating opt-out signals that meet the requirements of the CPRA and future agency regulations. The current digital ecosystem features a broad array of controls and signals, none of which clearly meet the requirements specified under the CPRA. Entering the next era of U.S. state privacy laws, new signals are likely to continue to proliferate and expand across new technologies and platforms, including an offline context in IoT devices and full connected vehicles. We therefore encourage the agency to engage directly with regulators in other jurisdictions, particularly Colorado and Connecticut, to develop an authoritative, multistakeholder process for the designation of qualifying opt-out preference signals as they are developed and refined.

**MS. HURTADO:** Thirty seconds.

**MR. LAMONT:** Consumers and businesses alike will benefit from certainty as to what preference signals meet the requirements under various state privacy laws.

Thank you for your time.

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

Our next speaker will be David LeDuc. Mr. LeDuc, please raise your hand. Thank you. Okay. Mr. LeDuc, you have seven minutes to speak. Your time starts now. You may speak.

**MR. LEDUC:** Good afternoon, CPPA board members and

staff. My name is David LeDuc, and I am the vice president for public policy at the Network Advertising Initiative, or the NAI. The NAI is the leading self-regulatory organization for advertising technology. For over twenty years, we've promoted digital advertising by maintaining and enforcing high standards for the collection and use of consumer data among our member companies. We appreciate the opportunity to provide input prior to the rulemaking process for the CPRA.

With five comprehensive state consumer privacy laws expected to become operative in the next eighteen to twenty-four months, and many more states considering new laws, we're facing an inconsistent set of rules that are likely to confuse consumers and create a desperate set of obligations that makes compliance extremely difficult for businesses. We therefore urge you to seek a collaborative approach in developing -- implementing regulations, and specifically, to work with other states to harmonize the requirements to the greatest extent possible.

Colorado Attorney General Phil Weiser recently expressed a commitment to harmonize his state's regulations with other states, and we hope that you'll engage in a dialog with Colorado and other states' enforcement officials to maximize consistency with

respect to the implement -- implementation of legal regulations. This coordinated approach can greatly benefit consumers in California and across the country and businesses that need to comply with disparate legal requirements. This will also be the overall benefit of the California economy and the U.S. economy, both of which are increasingly driven by data-driven innovation.

I'll be focusing my brief remarks today on CPRA's requirements around opt-out preference signals, which have been talked about extensively already. These generally refer to browser-based signals either deployed natively or through as a plug-in, device settings, or other mechanisms that communicate a signal to a business a consumer's choice to exercise his or rights to opt-out as provided by the CPRA and potentially and hopefully aligning with other similar state laws.

The NAI has a long history of promoting consumers' ability to exercise choice over uses of their data for digital advertising. Enabling consumers to express their preferences and exercise controls through easy-to-use choice mechanisms is a foundational element of tailored advertising that we have championed for decades. The CPRA provides the opportunity for businesses to either provide for a direct opt-out link on their digital property or to honor automated opt-out preference

signals.

While the NAI members already honor this direct consumer opt-out through do not sell links, we believe that most NAI members would also honor opt-out preference signals that represent clearly-expressed choice by a consumer. Broad and consistent recognition of these signals therefore would help to minimize confusion among consumers who deploy such mechanisms. Fortunately, the CPRA provides valuable protections to enable effective implementation of these signals, including the following.

First, a consent requirement for consumers to enable opt-out preference signals. For this, the CPRA defines consent very specifically, seeking to ensure that consumers knowingly and intentionally turn on an opt-out preference signal.

Two, a specific requirement for regulations to ensure that the manufacturer of a platform browser or device it sends an opt-out preference signal cannot unfairly disadvantage another business.

And three, direction to the agency to develop regulations that provide for reconciling differing preferences expressed by the same consumer to the same business.

These are three critical elements to deploying signals effectively. We urge the agency to develop

regulations that elaborate on these important priorities by doing the following. First, provide a requirement that any signal activated by a consumer is clearly communicated to businesses as a consumer opt-out request consistent with the opt-out rights established by the law. As Mr. Lamont mentioned, there are dozens, if not more, signals already in the marketplace, and most of these, if not all of these, do not clearly align with the opt-outs -- the legal requirements in the CPRA. In doing this, the regulation should avoid development of prescriptive technological standards, however. Instead, they should provide room for signal providers to customize their mechanism for the receiving businesses providing for them to be turned on and off by consumers within a settings menu.

Second, prevent unfair market disadvantages by establishing a process for opt-out signal technical -- signal, technical, and operational specifications to be submitted for review by the agency. This process should also include ongoing review by the agency to periodically evaluate and test approved signals to ensure that they continue to be administered fairly. To insist in the review -- to assist in the review process, it is essential that the agency also seek input from stakeholders, particularly those businesses to which the

signals are directed.

And I think Mr. Lamont also made a good point here regarding alignment with other states in this effort to try to provide for a group process -- a coordinated process, and we think that would be a very good idea as well. The agency should refrain from seeking to promote a singular opt-out signal, and instead should allow for various platforms and technology providers to develop signals that work effectively for their platforms and for their users.

Third, clarify that application of choices made via the signal applies only to the browser or device from which such signal is made, or in some cases, could be applied more broadly to a consumer if that consumer is known to the entity. The regulations should clarify that businesses are neither required to collect additional data from consumers to apply to opt-out more broadly, nor require steps to tie pseudonymous identifiers to known consumers in cases where the businesses do not already perform such practices.

**MS. HURTADO:** Thirty seconds.

**MR. LEDUC:** And fourth, the agency should clarify how a business may be able to prompt a user to disregard or override a signal. For instance, in cases where that business has obtained an opt-in consent to share the

consumer's data in accordance with clear terms provided by the businesses to the consumer. This is increasingly a challenge as more and more publishers and advertisers are engaging with their consumers and gaining their consent to use their data for advertising and for other purposes.

In closing, thank you --

**MS. HURTADO:** (Audio interference).

**MR. LEDUC:** -- again, for the opportunity. We appreciate it --

**MS. HURTADO:** Thank you.

**MR. LEDUC:** -- and look forward to engaging further.

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

Our next speaker is Chris Pedigo. Please raise your hand. Thank you. Okay. Mr. Pedigo, your time -- you have seven minutes. Your time starts now.

**MR. PEDIGO:** Great. Thank you.

Hi. My name is Chris Pedigo. I'm the senior vice president for government affairs at Digital Content Next. DCN is the only trade association that exclusively represents publishers and focuses on the digital future for thousands of trusted news and entertainment brands.

I'd like to first discuss how business practices are altered when a consumer exercises her choice to opt-out, and then second, how she technically makes this choice.

First, when a consumer opts out, the website or publisher cannot sell the consumer's data to a third party and should pass along this signal to any company which may have code on the app or website. So going forward, the consumer's data can only be collected and used by the publisher and its service providers, service providers which are contractually obligated to use data only on behalf of the publisher to deliver the requested service and not for any secondary purpose.

For instance, a news publisher and its service providers may use a consumer's data to remember a (audio interference) subscriber's information or conduct analytics on this usage of the site or the app. These types of uses are clearly in line with consumer expectations. They facilitate the trusted direct relationship between the consumer and the publisher, and we are pleased that the law does not limit this direct use by the publisher as it would harm its business.

With this dynamic in mind, Section 1795.135(f) of the CPRA stipulates that any third party company which receives the opt-out signal must immediately limit their use of that consumer's data to that of a service provider. We're very supportive of this provision for several reasons. It puts the onus for compliance on the company collecting data. It would be impossible for

publishers to audit the data practices of all the third party companies in the ecosystem. Another reason is that this section clearly lays out what companies can and cannot do with consumer data, thus, it avoids the need for publishers to renegotiate hundreds or even thousands of contracts. These contract negotiations can be lengthy, expensive, and they take resources away from the core business of creating news and entertainment.

More importantly, as you can imagine, a few large tech companies could and have previously used their market dominance to negotiate special terms in an effort to avoid the impact of privacy law. In short, we believe this section of the CPRA recognizes the complex and dynamic nature of the digital ecosystem, and we urge you to rebuff any attempts to undermine it.

The second point I'd like to discuss are the two methods by which consumers can opt-out. One, obviously is the do not sell button on a website. The other is to use a global privacy control, which persistently sends an opt-out signal to every website, app, or third party company that could potentially collect that consumer's data. The CCPA allows for authorized agents to send these kinds of opt-out signals, and the CPRA further clarifies this functionality.

We believe global privacy controls are important

because they could give consumers an easy way to opt-out of website tracking so they don't have to click on the do not sell button on every website or app they visit. We've seen nearly 80 percent of Apple users make this choice not to be tracked. By aligning with users' expectations, industry might even be able to (audio interference) consumer trust.

And publishers have an opportunity to enhance their advertising options as they can target advertising based on direct subscriber relationship data contextually and through other forms of privacy-friendly advertising. In enhancing consumer trust and the value of direct trusted relationships, this law provides opportunity for publishers to capture some of the ad revenue growth as small businesses and large seek out new customers.

We are concerned, however, that some will attempt to undermine the effectiveness of global privacy controls in several ways. Some on this call have suggested that the consumer should be required to take specific action to confirm or authenticate the signal. We believe this runs counter to the CPRA and the purpose of global privacy controls, which are meant to reduce friction and rapidly align with consumer expectations without requiring additional data or effort. We believe the CPRA allows these signals to be turned on by default, especially to

the extent that the service markets itself as a privacy-enhancing tool. That said, we are concerned that browser or device companies, particularly those with market power, may seek to promote their preference signals to unfairly favor their own business.

In closing, as you prepare draft regulations for the CPRA, I urge you to do two things. One, ensure that global privacy controls are easy for the consumer to use. Two, I urge you to reaffirm the text of the CPRA which stipulates that a third party must revert to the role of a service provider when a publisher or user agent communicates the consumer's opt-out signal.

I appreciate the opportunity to speak today and look forward to working with you in the future. Thank you.

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

Our next commenter will be Sebastian Zimmeck. Thank you. Okay. Mr. Zimmeck, you have seven minutes. You may begin now.

**MR. ZIMMECK:** Thank you very much. My name is Sebastian Zimmeck. I'm an assistant professor of computer science at Wesleyan University, and I'm one of the initiators of Global Privacy Control. And I will make it very brief. So I would like to make, you know, four points.

First of all, I think we need privacy preference

signals like GPC. You know, there was a study by Consumer Reports, and was mentioned here before, that showed that out links -- do not sell links -- are not sufficient. They can work on individual sites, but they don't allow consumers to opt-out, you know, broadly. It's just too many websites that users visit, and the solution to that is privacy preference signals at the browser level.

Now, the implementation for these privacy preference signals can be actually the same as for do not sell links. There does not need to be any difference. So when somebody clicks on a do not sell link, that can have, from a technical perspective, the exact same result as of somebody (audio interference) sends a privacy preference signal. So first point, we need privacy preference signals.

The second point, they should be mandatory as currently if the interpretation of the room. We have seen with do not sell -- do not track -- that voluntary, you know, appeals here did not work in the past, and so to give consumers a right that is really effective and efficient, it should be mandatory. That's the third point -- or to the third point.

Sometimes I hear that privacy preference signals do not represent the wishes of the user. So you know, it's

said, okay, it cannot be owned by default because the user does not know about it. And you know, we are doing research here at Wesleyan that actually designs interfaces and designs solutions so that users can be made easily aware of these signals. For example, there are tours initially when users can start the browser, and they can reference, you know, privacy preference signals like GPC. And I would also argue that most users are actually not aware that their data is being sold, and so you know, I would argue that most users do not agree actually with that as a default option.

Now, I want to address one other point that I sometimes here specifically related to Global Privacy Control as we have designed it, which is that it is related to all sites, and that's not the case. So it can be sent to all sites, but it can be also sent to individual sites. And so if a user wishes to only send their -- out to certain sites, they may certainly able to do so on their browser extensions that implement GPC that are doing that.

One other point on this, GPC is designed in a way that services that receive the signals do actually not need to keep track of state. So every time a website is being accessed, they will receive the GPC signal, and that actually makes compliance fairly easy. They do not

need to store the signal on their end. So privacy preference signals can be designed in such a way that they represent the user's wishes and that, you know, it is easy for sites to handle.

However, I do think -- and as my fourth point -- is that business models are impacted by, you know, by users, and so I think that is certainly something that, you know, publishers and other services need to think about. But whenever I go on industry conferences, you know, I remember one specific instance where I went, and I feel that there are many in the industry who actually understand us now and who are willing to evolve their business models.

You know, I remember one specific instance where a panelist said, yeah, you know, if you don't want to have a do not sell link on your site, maybe don't sell, you know? And so I would encourage, you know, all the advertisers in the industry to evolve their business models, and you know, give users a choice -- a true choice -- to make the privacy choices that they would like to have.

That said, I'm very happy if anyone, you know, needs assistance -- you know, technical assistance or has questions about this, you know, to interact with anyone willing to do so. Thank you very much.

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

Our next speaker, and last speaker for this session, is Aram Zucker-Scharff. One moment. Okay. Mr. Zucker-Scharff, you have seven minutes. Your time starts now.

**MR. ZUCKER-SCHARFF:** Hello. I am Aram Zucker-Scharff, lead privacy engineer for The Washington Post and senior solutions engineer for our Zeus advertising technology group, which serves over a hundred news sites. I also cochair the W3C's Community Group focused on private ad technology. I led and lead The Washington Post technical work around complying with California privacy regulations, and today, I'm speaking on behalf of The Washington Post.

The Washington Post was able to seamlessly roll out CCPA compliance for our California customers. When it became clear that the United States Privacy API, or USP API, as defined by the Interactive Advertising Bureau, the IAB, would become the industry standard for publishers and advertising systems. We were quick to adopt it. It is encouraging that a user with a little technical expertise can interact with and understand the output of the USP API. The idea of the technical signal warrants further exploration as it could have an adverse effect on businesses.

Advertising is one of the main streams of revenue at

The Washington Post. In the world of digital display advertising, we count load times and the time to first ad shown in milliseconds and have found that every millisecond counts, and adding extra loading time can have significant cost implications. Handling multiple technical signals not having a signal standard and instead processing multiple such signals, any of which could be built on technology that itself introduces a delay, would be a significant burden for publishers. It would mean extra code on page, engineering hours to build and maintain that code, and depending on the shape of that technology, additional delay as we waited on a response from the system. That is why it was crucial for me to be involved with the group that created the Global Privacy Control.

So many of the potential pitfalls and problems that could come out of a technology-based control were avoided in its creation. It does not require complex negotiation within API; it does deliver a promise, a technical concept in JavaScript, which could cause us to anticipate a delay in response; and it does not require complex calculation or decoding. When the GPC specification was ready, it was easy and straightforward for us to implement it. The entire change that was needed to support GPC on The Washington Post was seven lines of

code, less than 160 characters.

I'm prepared to show the actual code we have actively on our website right now to make clear the low lift for implementation. When this code runs, it sets the response in our systems to follow the users opt-out preference and is picked up by every relevant piece of ad and tracking technology on the page and either alters their behavior or is passed downstream the same as a manual opt-out process. The Washington Post takes these seven lines of code and has integrated them into our CCPA compliance mechanism that processes user status with the USP API. This happens on every applicable page of our website. Once this code runs and processes the signal, it is available for any other system that might need to know about a user opt-out. This setting of the USP API in this way passes the signal to all downstream providers, who can then comply with it.

The code easily alters the state of the techno -- toggle we provide for California users. It displays that they have selected do not sell mode and makes it visible that the user has selected it. We think of it as a robot for clicking that toggle. With the GPC process, the opt-out actually occurs even faster than it would normally. Of the ways we handle compliance, GPC, in our engineering experience, has proven the fastest and most

straightforward. We also can see the GPC HTTP header on any request where the user has it on and make a decision about how to handle it before the page even loads.

Our experience shows it is important to have clear, fast, and transparent ways for a user to opt-out and for a site to receive that opt-out. Because the user's privacy setting and the GPC signal itself are available on every page, it can be easy to note that the user is detected, and we have a variety of options to act on that. We can restrict particular technologies, display the user's opt-out status, and make privacy-compliant ad calls as close to instantly as we can get.

Our hope in speaking here is to make clear our experience implementing the California Privacy Law and the ease of use of the Global Privacy Control for opt-out. As rulemaking is being considered, we think that what we have here described is the required characteristics for a technologically-appropriate signal: fast, clear, and easily integratable into existing practices.

We believe these processes make -- or these properties -- make GPC a signal in the best interest of our readers, ourselves as a publisher, and the ad technologies we collaborate with, one that can be used to understand an opt-out under CPRA, and we wanted to make

our experience of early adoption clear and urge continued support of this methodology. We appreciate the opportunity to speak here and are open to any questions.

That is the end of my comments. Thank you.

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

**MR. SOUBLET:** I would like to thank all of our presenters during this last session on consumer's rights to opt-out. We are now going to have a break before our last session, which will begin at 2:30, and that's on Consumers' Rights to Delete, Correct, and Know. You can feel free to either leave the video on or leave it -- the conference -- open, or log out now and come back in when we start that session that, again, begins at 2:30. Thank you.

(Whereupon, a recess was held)

**MR. SOUBLET:** It's now 2:30. I'd like to welcome you back to the California Privacy Protection Agency's May 2022 Pre-Rulemaking Stakeholder Session. I'd like to also remind you that the sessions are being recorded.

This session, which is on Consumers' Right to Delete, Correct, and Know, speakers that are scheduled for this current session should be signed in to the public Zoom link using the name or pseudonym and the email they provided when they signed up to request their speaking slot.

If you are participating by phone, you will have already provided your phone number that you'll be calling from so that we may call on you during the pre-appointed speaking slot. Note that your name and phone number may be visible during the live session as well as in our subsequent recording.

Speakers will be called in alphabetical order by last name during this window, 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 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'll have seven minutes to provide your comments. In order to accommodate everyone, we will be strictly keeping time, and speaking for shorter than the length of time you're allotted is just fine. When your comment is completed, the moderate -- 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're also welcome to raise your hand during the portion at the end of the day set aside for general public comment.

Finally, you may also send us your comments via physical mail or email them to regulations@cppa.ca.gov by 6 p.m. tomorrow, Friday, May 6th.

California law requires the CPPA to 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 the topic of Consumers' Right to Delete, Correct, and Know, 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 we noted, the moderator will call you in alphabetical order by last name.

We'll now move to hear comments on the topic of Consumers' Right to Delete, Correct, and Know.

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

**MS. HURTADO:** The first speaker for this session is going to be Andrea Amico. One moment.

Okay. Ms. (sic) Amico, you have seven minutes to speak. Your seven minutes starts now. Ms. (sic) Amico?

**MR. AMICO:** Am I audible?

**MS. HURTADO:** Yes.

**MR. AMICO:** Fantastic. Thank you.

My name is Andrea Amico. I'm the founder of Privacy4Cars. We are the first and only privacy tech company dedicated to identifying and solving the growing provocations caused by vehicles. We've always offered tools and resources for free to consumers and we'll always continue to do so. Including last year, we created a subsidiary called Privacy4Cars California, LLC specifically for the purpose of filing data subject requests on behalf of California consumers.

So the topic for today is right to delete, but for cars, I think we should really be talking about obligation to delete, and the reason is because by the time the consumers reach out to us and say, hey, I think I left my data in my car, it's too late. Because to delete the data in cars, often you require physical access to the vehicle, and especially in this market where vehicles sell really fast, it's too late.

This is a massive issue because more than four out of five cars in California were resold last year containing the data of the previous owners and their

families, including minors, by the way. Among those, we also can count some celebrities. I recently met the new owners of vehicles driven by residents in Hollywood, and we've been told where they like to go to restaurants, what their phone numbers are, what their home address is, and the garage door codes to their mansions. This happens not only to celebrities; this happens to everybody. We don't think that's right.

Now, fortunately, December 9th there's going to be the new safeguards rule, so hopefully consumers start to enjoy some safeguards, but I hope that the commission will pay attention to the issue that sometimes it's too late when data is stored in physical devices like vehicles.

Also, we're going to be talking about obligation to know as opposed to right to know because when we send California consumers to forty dealerships -- large, reputable, great dealerships -- and they ask, hey, is the car that just drove, can it collect data, and is it true that the companies can actually sell the data through data brokers and insurance companies? Less than one in ten dealerships said yes and yes. That is a stark comparison with -- last week I was at the conference in San Diego, and there was another executive from a bank, and he was bragging how their cars can now collect 1,100

data points per second from consumers.

This is also stark comparison with the fact that in California last month a lawsuit was filed -- a class action was filed against a data broker that specializes in vehicle data called Otonomo because they allegedly collect data from tens of thousands of consumers in California and millions nationwide without the proper authorization. So what that is -- when consumers contact us, and you know, they click the button on our website that says, hey, I want to assert my rights, can you please file data request? Here's some things I think this commission would like to hear.

So very often, we get (indiscernible) answers, even from companies that typically have great (indiscernible) privacy. Apple, for instance, they'll tell consumers, just go in the privacy policy and you can read about Apple CarPlay, and it'll give you a new platform, and you can delete your data. But unfortunately, there's no section in Apple CarPlay. There's no section on either the privacy policy or the portal, so those consumers have no idea what they just collected from them; they have no ability to delete the data.

The same thing, by the way, happens with Google. We know that Android (indiscernible) can collect more than a hundred data points per second (indiscernible); like

consumers cannot protect themselves.

Other things that we see is that companies tend to keep us out of the loop. So we register our agents, customers appoint -- the consumers appoint us, but then companies refuse to interact with us, and they go straight to the consumer. I'm very glad that Consumer Reports filed a comment saying how this is completely (indiscernible). That's friction. It is the end result, and most consumers drop off from the process, and they cannot get their data deleted because they have to go through extra steps. They appointed us to do it; companies refused to do it. I think this practice should be banned.

We also see a lot of companies using the excuse of anonymized data to not respond. This is very common, especially with the brokers. They sit on massive troves of geolocation data that pins and pins and pins on people, what they're doing, detailed profiles, biometrics, and then they say, well, this is not Andreas' data so we cannot really delete your data. Well, our perspective is that if the data can be used to easily reanonymize people, or for instance, we seen the Otonomo lawsuit, but you're refusing to take action to protect consumers? Maybe you shouldn't have the right to do that in the first place.

So I am super grateful for the opportunity to speak to you today. I'm very passionate about the issue of privacy in vehicles. We think that this is a massive emergency that consumers are facing to get more than two million California families are data breached every year just because they sell a car or because their vehicle is repossessed or because it's part of an accident.

I hope that the commission will continue to look into this and remain available to you and to anybody else that is on the line here today. We're happy to share facts and figures and studies so that policy and action can be based on facts and not just on opinions and lobbyists. Thank you very much for the time.

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

Our next commenter will be Johannes Ernst. Mr. Ernst, you have seven minutes. Your time starts now. You may use your camera if you choose. You're muted, Mr. Ernst.

**MR. ERNST:** Sorry.

My name is Johannes Ernst. I'm a technologist and entrepreneur in Silicon Valley. And I will share one slide here if I can. I have three points to make.

Number one, we talk a lot about the costs that the new data rights we all have in California, including

businesses. I would like to mention that they also create many new business opportunities for innovative companies in California, and that is fundamentally because as personal data becomes available for more people, specifically the consumer, then the -- then just the company that has collected the data -- a new asset has become available for consumers to use as the -- as a piece, and that enables more choice, more innovation, and new business models not based on surveillance. So there's an upside to data rights.

Secondly, we have been -- at my company, we have been implementing open-source software that can help consumers visualize and use their personal data that they have obtained under the relevant laws, and as we have done that, we have found many, many issues with the implementation of data access by various companies. Some of them reach from the really mundane ones (indiscernible) by somebody somewhere to something that is more systematic in terms of companies perhaps not being as willing to provide the data as there is supposed to be another law. And I give you -- on behalf -- because for our own purposes, we have started tracking these issues with an issue tracker at a -- at the website that is very rudimentary but it is just there to collect them, called accesstracker.org.

To give you an example of what kind of issues we have been encountering, a credit union, for example, responded to a request that only one of the -- the primary account owner of an account may make a data access request on anybody who's on the account. That doesn't seem to read quite right. A credit reporting agency reported that they have thirteen fields containing thirteen different email addresses on a consumer, all of which were blanketed out with stars, which doesn't seem to be right. And a mobile phone carrier says, according to their privacy policy, that they collect and sell location data, but when the consumer in this case asked for the location information to be provided to them, they said they could not do so.

So there is many kinds of issues at all sorts of levels, and it is really difficult to aggregate them and see them because they only occur individually, one consumer at a time attempting to exercise their rights. So we would suggest that you may want to consider setting up a crowdsourcing process of some kind, and maybe accesstracker.org or something like that could be the seed of that, where consumers in California that run into various issues can essentially report that that would help the companies themselves in figuring out what actually works about the processes, and it certainly

would help in focusing investigators of various kinds, including your agency, to see where to look.

And so finally, the third -- the point I would like to make is that the process, in our view, for exercising data rights -- not just the right to know, but the other rights as well -- should be standardized and become automatable for software run by the consumer. And the reason for that one is that if hundreds, or perhaps thousands, we don't actually know, of companies have our data in various ways, there's no practical way for the consumer to go all -- to all of them and run through a custom process with each one of them, but this is something that is certainly very automatable with software.

And would like to point you to the datarightsprotocol.org in case you are not aware of that yet, which is a project spearheaded by a Consumer Reports to write an API -- to implement an API that allows software to exercise do not sell, as well as data access and other requests. And these are my comments. Thank you.

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

Our next commenter is Maya McKenzie. Okay. Maya McKenzie, you have seven minutes. Your time starts now.

**MS. MCKENZIE:** Thank you.

Good afternoon, Executive Director Soltani and other members of the California Privacy Protection Agency staff. My name is Maya McKenzie, and I'm technology policy counsel for the Entertainment Software Association, which is the trade association representing video game publishers and console makers. Thank you for the opportunity to testify today.

Our industry has long supported providing parents and gamers transparency and choice about how their or their child's information is used in connection with video games. It's also our intention and strong emphasis on -- we have a strong emphasis on providing and maintaining a safe online environment for all. So ESA supports the right of consumers to correct inaccurate information, however, there must be reasonable limits on that right to protect against fraud. The correction right can be abused by bad actors to evade detection gain unauthorized access to an account or otherwise facilitate unlawful or malicious conduct.

Specifically in the context of video games, a bad actor who was being banned from a game for harassing other players, for instance, or violating the game's terms of use, could request the correction of their IP address, user name or other personal information,

including substituting that information with fake data to circumvent anti-fraud, anti-cheat, and other detection systems that prevent such players from attempting to make new accounts.

For this reason, we request the California Privacy Protection Agency develop regulations that prohibit fraudsters and other bad actors from attempting to use the correction right to undermine the security or integrity of the service or facilitate their own lawful and malicious conduct. Specifically, the regulations should clarify that a business may deny a correction request when it has reasonable belief that a consumer's exercise of such correction right undermines the security and integrity of the service or facilitates fraud, unlawful, otherwise malicious conduct.

We have suggested draft language in our written comments. Happy to provide under separate cover. But this clarification is necessary to maintain consistency with the plain text and clear intent of the CPRA, which allows businesses to deny requests that are not verifiable, and also recognizes the need to balance the rights of consumers with the need to protect others and discourage unlawful activity. Further, this language is supported by the current CCPA regulations and commentary published by the California attorney general when such

regulations were published.

And if I may, I'd like to make comments on two other issues. It's also important that any technical specifications for the voluntary opt-out preference signal are consistent with existing children's privacy laws and reliably convey a parent or user's choice. On this issue, we request that the CPRA regulations require a business to honor a preference signal for children under thirteen only if such signal satisfies COPPA the standard for verifiable parental consent, and that such regulations not include a technical specification to determine a consumer's age.

Under COPPA, the federal children's privacy law, any business with actual knowledge that a child is under thirteen, or an operator of a child-directed site, is required to obtain verifiable parental consent prior to the collection, use, and disclosure of such child's personal information unless an exception applies.

COPPA preempts any state action that imposes liability for commercial activities regulated by COPPA, namely, obtaining verifiable parental consent when the state law is inconsistent with the treatment of commercial activity. And as detailed in our written comments, any technical specification that signals age will contradict clear, long-established Federal Trade

Commission guidance and ultimately is likely to prove too unreliable to effectively promote the CPRA's goals.

Finally, we request that regulations clarify what constitutes dark patterns by aligning with the Federal Trade Commission's robust taxonomy of userface -- excuse me -- user interface designs -- that the commission has deemed are unlawful as unfair or deceptive practices. Through enforcement actions and guidance, the commission has identified the following practices as unlawful: buried language that obscures material disclosures and terms, poorly-labeled hyperlinks that hide material terms from consumers, trick language that confuses consumers, and bait and switch practices. The regulations should align with such guidance and hold consent is not effective under the CPRA when businesses obtain consent using such unlawful practices.

That concludes my remarks today. Thank you for your time. We're happy to continue working with the agency on these regulations.

**MR. SOUBLET:** Thank you.

**MS. HURTADO:** Thank you for your comments, Ms. McKenzie.

Our next commenter will be Tracy Rosenberg. Tracy Rosenberg? Thank you. Okay, Ms. Rosenberg, you have seven minutes to speak.

**MS. ROSENBERG:** I need to --

**MS. HURTADO:** You need more?

**MS. ROSENBERG:** Yeah, just getting the controls in place.

**MS. HURTADO:** Okay, your seven minutes starts now.

**MS. ROSENBERG:** Thank you. Good afternoon, Agency and Executive Director Soltani. My name is Tracy Rosenberg. I'm speaking on behalf of two organizations, my own which I direct, Media Alliance, which is a Northern California Democratic communications advocate, and also, Oakland Privacy which is a citizen's coalition focused on protecting the right to privacy. I'm going to speak primarily on the section regarding right to know, right to correct, and right to delete, with a couple of additional comments at the end.

One of the questions that the Agency had asked was regarding how often a consumer may ask to correct inaccurate information. Our perspective on that is there's no doubt that inaccurate information increasingly presents troubling issues for consumers as computer-driven decision-making processes grow ever more ever present in inaccurate PII, whether caused by identity theft or sloppy data collection practices, and can cause consumers to be punished in a variety of ways. So while we are sensitive to the fact that businesses can face

some level of administrative burden, we are really reluctant to constrain the ability to have incorrect information removed on any sort of extensive basis.

We want to suggest that the Agency might want to consider the different kinds of inaccurate information that may be present and impose a specific and more liberal protocol for certain kinds of essential information relating to finances, health information, criminal/civil legal information that can have significant impacts on consumers. There's obviously a tension between the business desire to streamline processes, but there is a fundamental right for consumers not to be denied significant life opportunities due to incorrect data about them.

Secondly, you asked when businesses should be exempt from requirements to provide consumers with a right to know, right to delete, or right to correct under disproportionate effort or accuracy claims. Our position is that for consumers who are asking to correct information that is, in fact, not wrong, the consumer should be offered the opportunity to simply delete the information if they believe that it is incorrect. There is for most private individuals no journalistic or public interest concern and no private person should be forced to keep information on their online profile if they don't

want it there.

When it comes to effort, while we're open to the ability of businesses to request extensions for particularly expansive information requests, fundamental rights that are granted to consumers under state law should not be subject to dismissal based sort of on it being a pain to accommodate them. The fundamental rights as declared under law are, ipso facto, not a disproportionate burden to businesses, or if they are, it is a disproportionate burden that the government has decided that they must bear. So we would ask you to be limited in your disproportionate effort exemptions.

The final item was about procedures that businesses should follow to prevent fraud in the correction of online information. We want to incur -- encourage you to look at established processes like two-factor authentication and secret questions for consumers and want to state that these preferences are much more preferable than biometric identification techniques which basically will create new and enhanced privacy risks under the slogan of verifying identity.

Finally, we wanted to speak briefly about publicly available information. We are hoping that the Agency will address problems or ambiguities in the exemption of publicly available information contained in CPRA. We are

concerned with the nature of a business' reasonable belief that information is lawfully available, especially as this relates to the data broker industry. We believe this can and potentially will be interpreted to mean any lack of specific information that data was obtained in an illegal fashion and encourage a sort of negligent disregard for hacked or leaked information that is casually sold or shared without permission.

What constitutes a business' reasonable belief that information is lawfully available? Does that have to be proactive knowledge, and in fact, the information is available or simply a lack of information that it is not? We believe it is contingent on the Agency to more clearly define the parameters of what a reasonable belief constitutes within the current sort of data broker and data aggregation landscape.

If I have two more seconds, I will also briefly mention that we continue to have concerns about the financial incentives for surrendering privacy rights contained in the CPRA, Section 1798.125. The nondiscrimination clause in CPRA does continue to leave the door wide open for a two-tiered system that will inevitably over time focus data marketplaces on low income consumers who will have to forego the economic damages of opting out. The stark reality for low income

consumers is that it is unrealistic to expect them to be able to absorb the value of their data in every single business transaction they encounter in the course --

**MS. HURTADO:** Thirty seconds.

**MS. ROSENBERG:** -- of their lives. So thank you for the opportunity to speak with you today.

**MS. HURTADO:** You're very welcome. Thank you for the comment, Ms. Rosenberg.

Our next and last commenter will be Jacob Snow. Jacob Snow, please raise your hand. Thank you. Okay, Mr. Snow, you have seven minutes to speak. Your time starts now.

**MR. SNOW:** Thank you, and good afternoon. My name is Jacob Snow. I'm a senior staff attorney at the ACLU of Northern California. I appreciate the opportunity to comment, and I want to thank everyone on staff at the Agency for their hard work to protect people's privacy in California and around the country.

In 1972, California voters amended the California Constitution to add an alienable right to privacy, and the voter guide for that constitutional amendment said the following:

> "Fundamental to our privacy is the ability to control circulation of personal information. This is essential to social relationships and

personal freedom. The proliferation of government and business records over which we have no control limits our ability to control our personal lives. Often we do not know that these records even exist, and we are certainly unable to determine who has access to them."

Those words from the voter guide in 1972 could have been written today, and they take on special resonance as we see personal information increasingly being used to harm, track, hunt, watch people and surveil them.

Consumer rights to know what information companies hold about them is a foundational value under the CCPA and the CPRA, and it operationalizes those constitutional rights and norms that have long been a part of the legal firmament in California for decades. I hope the Agency makes this lineage clear in its rule making and public education efforts as it begins its important work.

The Agency should also reflect on who the constituents of this privacy law are. Are the constituents of this law the people who are exposed to harm from the government and from companies who possess their personal information, or are the constituents the companies themselves who are collecting and harvesting information from consumers and amassing and selling people's most sensitive information to the highest

bidder?

As we all know, the CPRA and the CCPA -- CPRA amended the CCPA in 2020 to enshrine a trade secret exception in the law. Now this was the wrong decision. It placed the interest of companies in collecting and using people's information over the interests of people whose information was being used, and maintaining control over their own information on those consumers' behalf is a foundational privacy right. It allows people to live their lives free of surveillance, to flourish in their communities, to preserve their own safety, as well as their family's trade secrets, on the other hand, or corporate assets. The CPRA made a grave mistake in prioritizing speculative corporate assets over Californians' fundamental privacy rights, and the Agency can limit the damage of that mistake by promulgating regulations that ensure that trade secrecy claims are fully and robustly supported by evidence and narrowly construed.

Professor Rebecca Wexler has shown us in her article Life, Liberty and Trade Secrets that trade secrecy claims have been used to harm criminal defendants and to deprive them of access to information that is necessary to protect their lives and their liberty. The trade secret exception in CPRA only goes so far, however, and it

doesn't require a trade secret exception for automated decision systems.

The trade secrets exception in CPRA only exists for verified consumer requests, and as such, if a company had to disclose information about an unmade decision system for use publicly or to an agency, no verified consumer request would be required, and no trade secret exception will apply. I encourage the Agency to resist carve-outs that allow businesses to hold back information by claiming trade secrets, proprietary information, or that information is subject to nondisclosure agreements between parties, and therefore, cannot be shared with consumers.

One goal of automated decision-making regulations should be to improve the understanding that people have who are directly affected by the decisions that are made, but it's not enough to think merely an individual consumer. There's a collective societal interest in understanding how companies are making important decisions about people and ensuring fairness in those decisions, especially given the well-documented discrimination that grows in algorithmic darkness. Companies should not be allowed to escape scrutiny by claiming the commercial need to protect their intellectual property or other company information.

I'd also like to make a statement about the Agency's position on a federal privacy law in particular, preemption in a federal privacy law. The Agency should come out with a strong statement opposing any preemption in a federal privacy law. From net neutrality to police violence, it is foundational to our democracy that states, counties, and cities have the ability to listen to their residents and make policy changes that can protect the communities that they represent. A federal law wiping out state protections would be a bad deal for consumers that would put existing consumer protections, many which are state led and many which exist under California law today, on the chopping block. It would leave states bound by a federal law that could prevent additional consumer privacy protections from ever seeing the light of day.

Consumer privacy law in California will only get stronger over time, and those improvements which may be years or decades in the future should be guarded by this agency. State regulators could lose the authority to fine or sue companies that violate their laws, and all the work of this agency from making privacy choices easier for consumers to building a robust enforcement apparatus that can do its job of enforcing a law on behalf of 39 million Californians could all be wasted.

I appreciate the opportunity to comment. I look forward to continuing to work with the Agency in protecting Californian's privacy in the future. Thanks very much.

**MR. SOUBLET:** Thank you.

**MS. HURTADO:** Thank you.

**MR. SOUBLET:** That was our last speaker for the consumer's right to delete, correct, and null session. We'd like to thank all those who presented during this session. We're going to take a break now until our next session begins at 4 o'clock. That is the general public comment session, and we'll be back in just a little under an hour at 4 o'clock to begin that session. 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 132 to the best of my ability from an audio recording provided to me.

I have subscribed this certificate at Phoenix, Arizona, this 16th day of June, 2022.

Cynthia R. Piett

eScribers, LLC

--o0o--