MS. KIM: On behalf of the California Department of Justice and Attorney General Xavier Becerra, welcome to the seventh public forum on the California Consumer Privacy Act.

We want to thank Stanford Law School for hosting our forum today.

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

Today, our goal is to listen. We are not able to answer questions or respond to comments.

Before we begin, we would like to briefly introduce ourselves. My name is Lisa Kim. I'm a Deputy Attorney General of the Privacy Unit, which is in the Consumer Law Section of the AG's office.

MR. MAUNEY: And I'm Devin Mauney. I'm a Deputy Attorney General in the Consumer Law section.

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

MS. KIM: So we will begin in just a moment,
but I wanted to go over a few process points before we start.

Each speaker will have five minutes to speak. A member of our staff is keeping time with these yellow cards. And so we ask that you please be respectful of the timekeeper, as well as your fellow speakers today.

We are also audio recording the forum today, and will be transcribing the comments afterwards. So please speak slowly and clearly.

As with the transcripts of the proceeding forums, once they're available, they will be posted on our CCPA website. These you Power Point slides are also available on our website.

The front row here is reserved for speakers. So when you come up to the microphone, it is requested but not required that you identify yourselves when you're offering your public comment. You may sit in the front row so we can know who's about to speak, but if you would like to just wait in your seat, that's fine, too.

It would be helpful if you provide us a business card if you are speaking. But again, it's not required that you do so. And if you have a business card, you can just leave it in the front of our table right here.
We also welcome written comments by e-mail or mail. Our deadline for submitting written comments is this Friday. And the e-mail and mailing address is listed up here on the slide.

Bathrooms are right behind us. The women's restroom is right behind us, and the men's restroom is on the first floor. And we will be taking some breaks throughout the process today.

May I ask if there's any media present, if they could please raise their hand. I don't see anyone. Thank you.

So I just wanted to cover a little background on the rule making process. The rule making process discovered by the California Administrative Procedures Act. During this process, the proposed regulations and supporting documents will be reviewed by various state agencies, including the Department of Finance, as well as the Office of Administrative Law.

Right now, these public forums are part of our initial preliminary activities. If you can make it out on the screen, it's way at the very top of the red arrow. This is the public's opportunity to speak to what the regulations should address, and what they should say. We strongly encourage the public to provide oral and written comments, including any
proposed regulatory language, so that we can take that into consideration as we draft the regulations.

Once this informal period ends, there will be additional opportunities for the public to comment on the regulations after proposed draft is published by the Office of Administrative Law.

We anticipate starting the formal review process, which is initiated by the filing of a Notice of Proposed Regulatory Action in early fall of this year.

The public hearings will take place during the formal rule making process, and they will be live webcasts, as well as videotaped.

All oral and written comments received during the public hearings will be available online through our CCPA web page. So if you would like to stay in touch or informed throughout this process, this is our website. www.oag.ca.gov\privacy\CCPA. You can also sign up for our e-mail address at this web page.

Finally, the CCPA Section 1798.185 of the Civil Code specifically identifies areas for rule making responsibilities by the AG. The areas are summarized here in sections one through seven, so please keep these in mind when providing your comments today. I'll go through them quickly.
Number one, should there be any additional categories of personal information. Two, should the definition of unique identifiers be updated. Three, what exceptions should be established to comply with state or federal law. Four, how should a consumer submit a request to opt out of the sale of personal information. And how should a business comply with the consumers request. Five, what type of uniform opt out logo or button should be developed to inform consumers about the right to opt out. Six, what types of notices and information should businesses be required to provide, including those related to financial incentive offerings. Seven, what can a consumer or their agent -- I'm sorry. How can a consumer or their agent submit a request for information to a business, and how can the business reasonably verify these requests.

So at this time, we welcome comments from the public. If speakers want to come down to the front row, they're welcome to do so now or take the mike. Thank you.

SPEAKER 1: My name is (inaudible) Preston (inaudible) I'm with Common Sense Media, which is (inaudible) of the law organization founded by teacher here.

I just want to make a couple points to put
this law in context.

    The CCPA is not a perfect law. No one has
every claimed it is, but it's been critically
significant law for a number of reasons. First, and
most importantly, this is probably the strongest
advance for children's rights (inaudible) since the
Children's Online Privacy Protection Act passed in
1998. When that passed in 1998, some of the biggest
(inaudible) on the internet included Geo Cities, AOL
(inaudible) digital experience like our kids be growing
up today with something we just didn't understand at
all about.

    Some of the rights that kids have earned
under the California Consumer Protect Act is the right
to opt out or right to have an opt in to their sale of
their data by any tech companies for kids under 16, and
in the affirmative requirement that companies would
understand and not sell any data for kids under the age
of 13. So when these rights are enforceable in court.

    And I just want to take a moment and reflect
on why these rights are so important. First of all, we
are research organization, Common Sense Media, 98
percent kids under the age of eight have access
(inaudible) devices of their own. 72 percent of teens
today believe that tech companies use techniques to
manipulate them keep them online. We know this is true from the work with another Stanford graduate, (inaudible) Harris, Center for Humane Technology, which talks about the way many of the tech communities use techniques with (inaudible) psychology. They look at how to increase the attractiveness of sounds and visions with the idea of getting kids into addictive relationships with their technologies. No surprise, 56 percent of teens say they feel addicted to (inaudible) cell phone, and 68 percent of teens say the negative effect on their own generation.

Let's think about that for a second. There are reams and reams of social science research about how to sufficiently develop kids, the most effectively developed kids in education and parenting sect. But if kids are on media for nine hours a day, that's more time than they're spending in schools, probably more time than they're spending with their parents. And (inaudible) conducted on them, almost no research about what its affects are.

We know there are good things that come with technology, but we also know bad things that come with technology. So -- forgive me.

And in that vein, can you think of another product that is so persuasive, so pervasive in our
lives, there's so many bad effects which mix in with
the good effects, and it such a crisis of public policy
and a crisis of circulation of government, as well as
crisis of ethics and crisis of morality that these
companies that are pushing it.

So let's celebrate the CCPA for what they do.
It's incredible step forward. It's an example of
democracy can work. We've overturned with this law
some of the most insidious (inaudible) effects of this
company has ever -- this country has ever seen.
Technology companies have spent billions of dollars
over the last 20 years to ensure there's almost no
regulations on their product. They been successful
with that. And no money (inaudible) self-regulation.
They been incredibly unsuccessful at that, despite a
litany of promises from every CEO that self-regulation
is the way to go.

We seen the result in the series of scams.
YouTube is pushing completely inappropriate (inaudible)
kids, content to kids through using kids. YouTube is
also enabling, according to reports, networks of
pedophiles who are commenting on YouTube kids' videos.
Uber, Facebook sold the data of 126 million Americans,
or (inaudible) allowed to access it and pump this
information into our political process. What's perhaps
the most worrisome example of propaganda I can think of in recent times, Uber and Twitter are under investigation by law enforcement for invasive trapping of kids geo location in every piece of data kids have.

So the CCPA isn't perfect. But I ask this member what it is. It's a cultural sea change. It's a reflection by the California government that the system that this industry is out of control, and that the public wants immediate changes. Facebook (inaudible) 22 percent of Google (inaudible) that's less than half or about half of president, who is hardly a popular president.

So let's run around how important this is for kids. (inaudible) you for every time when you urge this law to be weakened, show your good faith by suggesting a way it can be strengthened. Show your good faith to users you really are trying protect.

In front of the DOJ staff, I want to thank you for your time. You're in a very difficult situation. Because as I mentioned, for 20 years, this industry has developed, almost without regulation. So you all are trying to have to pick up on that.

I will remind you, though, that the public is behind you, even 59 percent tech workers are behind you, and a clear legislative intent of this law was to
change the situation and get consumers, and especially kids new rights.

So I hope you remember that. And I thank you for your work.

SPEAKER TWO: Hi. I'm Eric (inaudible). I'm a professor at (inaudible) University School of Law.

I do agree with the last speaker that the CCPA isn't perfect (inaudible). I want to (inaudible) emphasis, however, on digital companies and (inaudible) data. As we all know, the law applies to off-lying companies as well, and thousands of them, if not millions, as well as to data that's non-electronic form. I know you're working on recovery employees cases of the law, not just how (inaudible).

I (inaudible) at the San Francisco (inaudible) and I want to follow up on comments with a procedural request that I learned since the passing of (inaudible) that I think there's a lot of people who are hoping that their office (inaudible) regulation, that you won't be eliminated to playing in the sandbox as defined by 1798.185. We obviously are (inaudible) talk about that. We're hoping that they'll talk about a lot of other things as well.

At the San Francisco hearings, I think you'll recall, (inaudible) talked about that I think everyone
talked about something else. And there's a lot of (inaudible) in the something else you might talk about as well. (inaudible) to me is how your office and the Legislature will divide the responsibility between the Legislature superintending the tested law, and the AG's office rules and will stand, clarify, and even (inaudible). Everything that I have seen, the Legislature respects the AG's office, will take the full benefit (inaudible).

So I ask to you is I hope (inaudible) in the regulation. There will be a target of wide range of topics.

Next thing I'll say (inaudible) responsibility. I'm not sure you (inaudible) so thank you for the work that you're doing, thank you especially for holding (inaudible) We appreciate the hard work that you're doing (inaudible). Thank you.

SPEAKER THREE: Good afternoon. Thank you for the opportunity to come. My name is Susan (inaudible) I'm an attorney at (inaudible) certified US and European Privacy Law.

The (inaudible) Law represents companies that serve California consumers that are working to (inaudible), to help them protect customers that are customers and privacy.
I would like to suggest some rules of clarification that could make it easier for companies to comply with the California Consumer Privacy Act in a way that protects the individuals.

The first rulings to verification of consumers' right to access data. Many commenters have discussed the potential risks associated with providing consumers with access to data about all individuals who are believed to be members of the same household. Under your authority to make rules for related to verification of a consumer's access requests, you may wish to consider a rule that provides access to household data only in cases where data is inherently collected or stored in the household (inaudible). For example, a database of household income, or record of overall household utility usage might well be household personal data.

For data to be broken down to the individual level of individuals who live in the household or the use of individual devices, no one individual should be considered verified to gain access to data about other individuals in a household. That limits some of the security issues, privacy issues and dangers that are otherwise inherent in the inclusion of household information, in the definition, which clearly has
function, but with respect to access to right stuff
we'll ask security.

The next comment relates to verification
(inaudible) access to personal information as well.
Under your authority to promulgate rules to facilitate
business clients and verify the consumer requests to
access their information, it would be helpful to
clarify that device (inaudible) alone without other
personal information are not enough to verify the
consumer's identity. This would help businesses avoid
providing consumers information to bad actors making
fraudulent access requests. Businesses that have only
these device identifiers also shouldn't be obligated to
collect additional information to verify consumer's
requests for access to personal information.

And relating to the definition (inaudible)
identifiers, in certain online transaction, unique
identifiers are used and disposed for purely
operational purposes. But if you read certain of the
definitions together, that could lead you to the
counterintuitive conclusion that those transactions are
the sale of personal information under the CCPA.

Using your rule making authority to clarify
the definition (inaudible) identifiers in order to
overcome obstacles (inaudible) and your authority to
adopt additional regulations to further the goals of the CCPA, you may want to consider clarifying that when unique identifiers, such as IP addresses, are used for purely operational purposes and not profiles, they're not serving functionally as personal information, and their disclosure should not constitute a sale of personal information with the CCPA. Because as long as all the parties that receive the identifiers are prohibited from using them for other purposes, regardless of what those parties do in other respects for businesses.

But in that context (inaudible) prohibited from using those identifiers for other purposes. The identifier are not really functioning as personal information and that shouldn't be a sale.

Thank you for the opportunity.

SPEAKER FOUR: Good afternoon. Thank you for the opportunity to (inaudible) residence of California and chief (inaudible) advertising technology company called Comcast, which is based in San Francisco, California.

We support the underlying (inaudible) of the CCPA, including transparency, control and accountability. In fact, self-regulatory (inaudible) conduct principals that third-party advertising
companies, such as Comcast, (inaudible) were founded on
those principals, as well as the concepts, such as
(inaudible). The fact that many aspects of the CCPA
align with (inaudible) existing software guidelines is
a welcome attribute of the law, and something we hope
your office would take into consideration.

But there are some materials (inaudible)
remain ambiguous and open to a range of interpretation.
We ask your office to provide guidance and increased
certainty of (inaudible) in ways that advocates
(inaudible) existing privacy practices that are also
technologically feasible. It is our hope that your
office will clarify the scope of specific definitions
of the CCPA and how it intends (inaudible).
Specifically, we ask that your office provides guidance
and clarification on the definitions on the personal
information, and sale that are included in the law.
These definitions are very broad and ambiguous as they
are (inaudible) address the important nuances
(inaudible).

In particular, we ask that your office issue
guidance on a different types of data, including
definition (inaudible) including emphasis on the
importance and value of (inaudible) instead of
(inaudible) identifiable (inaudible.)
For example, the interpretation of the definition of personal information is general, and it gives many different types of data on this (inaudible). But not all data included in that definition are the same. The range (inaudible) personal information definition is broad (inaudible) everything from remaining on Social Security number to (inaudible) generate (inaudible). There are dramatically different risk profiles associated with various types of data included in that definition. Distinguishing between the use of information and being directory tied to a person without enough data with (inaudible) information that is intentionally obfuscated and (inaudible) other information that tied that person that (inaudible) is very important. Acknowledging this (inaudible) encourage to choose to work (inaudible) information. Instead of information that is personally identifiable, this directly benefits the right to privacy that was given to you in California Constitution.

Similarly, the definition of "sale" (inaudible) different digital companies communicate with one another that are actually transact business. For example, as defined, sale (inaudible) includes the exchange of information and it is not the subject of the transaction. In market places that serve
(inaudible) which supports the (inaudible) data is often (inaudible) transaction, even when it is not the subject, it is merely (inaudible).

Thus, current definition (inaudible) while there is an exception provided for certain (inaudible) we do not believe that fully captures the way in which advertisers, and websites (inaudible). We also do not believe it is intentional drafters (inaudible).

So guidance provided by your office will be helpful to assist the marketplace to better understand how to properly (inaudible). Thank you for your attention and look forward to guidance from your office (inaudible) and aspects of the law, (inaudible).

MR. MAUNEY: Once speakers have already gone to the mike, you can leave the seats down in reserve area for those (inaudible) that would be great.

SPEAKER FIVE: So my name is (inaudible) Silverstone (inaudible) consultancy called (inaudible) I had the pleasure of being both in California (inaudible). Therefore, I'm subject of your (inaudible) both and (inaudible) unbelievable that they exist in the United States regarding privacy.

I want to start by say thank you. This is a huge step forward and because of the economy of the State of California, and (inaudible) six states are
virtually hoping this law, and three other states
adopting the law, and for the first time, we may get
the point trying to see that is perhaps in the
(inaudible) of the United States.

I want to talk first and mention some numbers
from CCPR. These are raw numbers. They are very
(inaudible). I would like for you to think what those
numbers mean (inaudible) for roughly around December of
2020. I will then talk about my experience as a
European. We (inaudible) complete the subject. And
finally, I would like to make a few suggestions
(inaudible) process, et cetera and to cite the
amendments currently under discussion.

I also (inaudible) CIPT and CIPM. I am
(inaudible) chief security officer for companies such
as Expedia, (inaudible) vice president of security and
privacy (inaudible).

So start with the numbers. So I think it is
very -- in the December 2018, there have been roughly
registered 60,000 complaints across Europe provided
nation (inaudible). Most of these were given by stated
subjects of all. And if you are wondering what the
average would be, it will be about 2,200 country,
because some countries Europe don't have 2,000 people,
but that's the average.
Since then, in (inaudible) saying due to the fact (inaudible) end of the year, the current count is over 100,000 complaints under process. That's an average of 3,600. The biggest (inaudible) of complaints have been number one, CCPT abuse of visual imagery, specifically in parts of Europe, you are pretty much disallowed to (inaudible) your employees use CCPT, unless there's a whole list of "unless".

And even picture the student ID card for the purpose of identification in an office might very well be restricted under the GDPR (inaudible) gender, religion sometimes, race, national origin, et cetera.

Number two, the gentleman (inaudible). The number two category for complaints, marketing poles.

And three category (inaudible), marketing e-mails. We're talking together about 100,000 complaints that we'll see the space of roughly six months for the population of Europe, which is comparable to the population of the United States. It mention what the big percentage the US population in California represents.

(Inaudible), which this law touches on, under the GDPR rule to announce notifications of possible or confirmed purchase (inaudible) 41,000 notifications of the regulators in the six months and (inaudible),
41,000 breaches, those 41,000 records. So we know how bad the situation is. Where as a year ago, people (inaudible) say certain.

And finally, (inaudible) authority in Europe (inaudible) average two investigations by themselves per country. But there are over 200 investigations in addition that were created by complaints. This roughly seven and a half percent. (inaudible) Thank you.

SPEAKER SIX: My name is (inaudible) counsel of a need to be internet company called (inaudible) communications.

And you know, I echo what everybody else has said (inaudible) important but, I hope that the office can take into account that the digital echosystem has many, many layers. And they're making one company up at the top, the Google, the Facebook, the Pay Pal, whoever, that deals with the consumer, there could be other 10 others behind that company that are assisting that company in providing service to the consumer. And the bill only addresses this top layer (inaudible) consumer. But we are providing services to companies who do.

And so we're uncertain what our obligations are. And don't think it's fair for a lot of (inaudible) these a huge (inaudible) of California
businesses uncertain of what their obligations are. We have spent the last two years trying to figure out our obligation under the law that actually does distinguish between a consumer-based companies and everybody else. The GDPR makes a really clear distinction between data controllers, those are the ones who determine the purposes of information be collected for purposes of processing, et cetera. They're the ones who (inaudible) consent from the consumers for collection of certain data and the processing of data, and then they can share that data with data processors as necessary to count the service performed.

And it's pretty clear that that's not the sale. Is it a sale if we give them the information (inaudible) web service (inaudible)? I don't know. Is it a sale if our customer gives us data to process in our analytic platform (inaudible) serve back up to them for their internal business services? We're making no money off of it, other than providing service.

So I'm going to encourage the office to think about this really critical distinction between the consumer casing in businesses and everybody else and what their respective obligations are, you know. And (inaudible) pretty clear, we also have a lot of time to figure out. We have to serve up data processing
addendums to our customers who say, we will only
process data per the, you know, purposes of you tell us
to process it for. But, here's the people you have to
go get consent from the consumer, not us.

We have no way of putting opt out button on
our website. We don't know who consumers are. They're
unknown to us. We have no relationship to them. We
tell our customers, you know, it could be a bad by
price by design if you can even give us that
information, you don't have to. And so there are a lot
of new ideas out there that could be used to help
California businesses understand what they're supposed
to do.

And lastly, I think the law is missing a core
concept which is consent. The GDPR law as it is, at
least, you know, says, hey, companies. If you're going
to collect data from somebody to provide a service, why
don't you tell them what you're collecting, the
purposes for which you are using data, and who you're
going to share it with. And so we have all spent two
years grappling agreements that spell each of those
out. You know, I reviewed a customer, the consent that
they give to their customer to make sure they
appropriate describe the data that we need them to
collect so that we can provide the service to them.
And it's all really helpful and useful stuff. You know, I don't know how you can avoid adopting some regulation that deal with this distinction between controllers and processors (inaudible) if a question comes up, and an enforcement action what's the court going do, we have -- how are they supposed to interpret, other than by going and looking (inaudible) which is place they can tag to to really understand what the difference, you know, the different obligations of the problem solvers.

So I don't envy your jobs, but I hope you can help the bottom layers end the difficulty (inaudible) what their obligations to, their customers and to the ultimate consumers. Thank you.

SPEAKER SEVEN: My name is (inaudible). I'm not a law student, I'm a regular citizen. So some of the legalese (inaudible). But I wanted to come here today and say first of all, thank you for (inaudible) that would protect our rights for privacy, especially on my end (inaudible), seeing what happened with the most recent election, data being stolen and used by foreign governments (inaudible).

I -- my family also grew up in an eastern country with communism, so we know the importance of privacy. Their phones were hacked by (inaudible)
underground for the actual news. So my family does
know the very important nature of this.

But I also wanted to say I have this personal
experience with privacy being breached where I was
e-mailed by a current password (inaudible) password and
the person e-mailing five (inaudible) saying they had
videotaped my (inaudible) website, all my contacts.
Because it was a real password that they had, I took it
seriously. And although it was a scam, it was of the
different nature of scam, because they actually did
have some personal information. So whether that was by
some website that I visited, and was not able to opt
out of having third party sell my information, or a
contact in an application that I had like a friend on
Facebook, who by being their friend and visiting on
other sites (inaudible) information.

I want to say thank you for doing something
about this issue. And I also wanted to request an opt
in version so that you are already opted out of any
kind of selling of personal information on a site that
you go to, and something that is very easily and
quickly read understandable, rather than a very long,
legalese document that (inaudible) privacy section,
which most people might skip over, (inaudible)

SPEAKER EIGHT: (inaudible) perspective chief
complaints officer (inaudible). We are (inaudible) in service business very seriously. And (inaudible) group today about how to clarify definitions and processes so we can continue to be in compliance and serious about practice. We have (inaudible) $30,000 across Northern California (inaudible) and seriously. But now we have very general rules to try and to capture a lot of (inaudible) information (inaudible) specific so we can do right by our members, as well as non-members who come to us (inaudible) as well.

In particular, we have what I refer to (inaudible) language. There is a large (inaudible) September position that were made (inaudible) saying that data is collected under (inaudible) or California (inaudible) that it is already protected under existing privacy laws, then this is exempted from of this (inaudible) new law.

Well, an awful lot of (inaudible) because we're in (inaudible) service has to do those things. All of our vendors that we share our data in order to accomplish transactions, all have the highest standards (inaudible) due diligence make sure that they're not going to breach the data (inaudible) understand confidentiality (inaudible) already.

So now we have a member comes to us and
knocks on our door come January 1st, 2020 and says, show me all the data you have on me. And we said, well, actually, all the data we have on you (inaudible) show you anything now. That's not going to go over well. So we need proper language indicating rules that tell us what is it we can tell people about how (inaudible) and what their rights are or are not, in addition to those rules in the new law.

That also is pretty much a theme (inaudible) talk about today is just give us specifics about how we can respond and how we can (inaudible) to stay compliant. There are a lot of different areas that touches on, including (inaudible) requests we have Department of Homeland Security telling us we have to keep data in perpetuity now because they want to be able to track, you know, bad guys.

So how can we get rid of data if we're not using it anymore (inaudible) keep this information to try to find bad guys? So (inaudible) specifics in here (inaudible) 1798.110, 1798.115 talk about data collected (inaudible). But it doesn't talk about how -- let me just go down the list here real quickly.

All right. So the information we shared with our service providers. We'll talk about service providers and our obligation. And some advice
(inaudible) service providers as sharing they're handling safely, we want to make sure that information security (inaudible) satisfies what this nuance says to ensure the information stays secure. Are we already doing enough (inaudible) set the standard (inaudible) today have been breaching by lots of different organizations (inaudible) everybody has had a say in how to establish industry standards. And that's what we follow. And we need to know whether or not this law is going change those standards or not. Again, because we want to do the right thing. We just need to know how.

As to the issue of non-identified information, IP addresses, cookies, (inaudible) of information that we come across as people comply to (inaudible) actually finish their applications, or we don't actually give them a loan (inaudible) information.

A lot of times, we don't know who these people are. Somebody who's knocking on your door says, I'm showing you everything you got on me, great. (inaudible) How am I supposed to go find all this (inaudible) information (inaudible) IP addresses. From a practical standpoint, how are we supposed to know who these people are if that is the only information we
have on them? This law talks about (inaudible) other
laws, other data (inaudible) into personally
identifiable information, great. (inaudible) You're
not going to make us go out and turn it into
(inaudible) already, so we need to know, are we liable
for that information or not?

There are other categories also, but not as
important as things like the names and addresses of
people who spend contracts with us. Are they
consumers? Do we have to do give all the information
to them? (inaudible)

Essentially, our ask is, give us scenarios
specific so we can -- give us rules to follow that we
can do the right thing in situations we actually
encounter when somebody comes and knocks on our door
and asks for information.

Thank you for your hard work. We look
forward to seeing (inaudible).

MS. KIM: If we can have everyone go for the
first time first, and if there's time (inaudible)
Thank you.

SPEAKER NINE: I'm Paige Barkley (phonetic).
I'm an industry analyst in (inaudible) where research
(inaudible) practices. And I over the last three
years, I've had a very strong focus on data privacy,
and data privacy communication. So in the regular course of my work, I work with a lot of software providers that either offer these types of solutions and also work with companies that are trying to implement practices.

So I think the main point I want to give today most important for this audience is to (inaudible). And I think the myth that's pervasive (inaudible) is that data privacy (inaudible) regulation somehow (inaudible).

And I strongly believe from my research and my line of work, that this is actually (inaudible) data privacy practices and giving controls to consumer when implemented correctly is not (inaudible). We talk about the new data era, how data is the new coin. It's the new currency. It's a business' most valuable resource and asset. (Inaudible) this is data been collected and controls in the pervasive business (inaudible) data is good, old data must even be better. So therefore, (inaudible) you have a philosophy that collect and analyze as much data as possible, no matter who it belongs to or where it came from, you can keep it forever (inaudible).

But if you look at regulations by CCPA, (inaudible) or data regulation, there's a common
business requirement underlying that. And when you
strip down these regulations, they're (inaudible) that
corporate environment is that you have absolutely
granular control of the data within your organization.

And what businesses came to realize is that
if you have this absolute control of your information,
there are numerous other (inaudible) benefits for your
business. In the data driven economy, when you're
trying to leverage information and use data to its
maximum value, when you have that control of
information, it has numerous other benefits. So you
need to be able to continually find personal data
associated with proper identity (inaudible) to retrieve
it or modify it as necessary. So that complete
granular control of data benefits the business
(inaudible) cases.

So if you look at proactive (inaudible)
enterprise like analytics, business intelligence, they
all cannot (inaudible) control of data that is
required.

So with strongly hold data, business can
agree to overall quality rather than quantity of your
data. So if you give consumers control and data
privacy, they may decide to opt out of certain data
sharing collection, the data they do provide needs to
be more (inaudible).

With stronger data control, you increase security and (inaudible) over time. Because it controlled require privacy (inaudible) control required to security breach, and their eventual PR impacts are incredibly expensive (inaudible) as a business.

With strong data control, you also have the opportunity to build trust and long-term profitable relationships with consumer (inaudible). Trusting relationships result in a longer lifetime spent with the business. So when you have trust and consumer (inaudible) to be done, they ultimately spend more over time (inaudible).

And finally, (inaudible) data access within an organization. So if initiative such as self-service analytics, (inaudible) able your internal knowledge workers to access and use data, the strong data (inaudible) allow you to very granularly control who has access and what and when and why. So the business' ability to control data will determine business' ability to innovate and adapt (inaudible) economic system and data (inaudible).

Data privacy regulation is forcing (inaudible) organization (inaudible) reconsider (inaudible) fundamental data (inaudible) practices.
And this a very positive thing. With regulations, such as GDPR that finally cause many businesses to actually have the funding (inaudible) to go and reconsider (inaudible). This is a good thing for both businesses and consumers, result in improvement business efficiency and improve customer (inaudible) over time.

So in conclusion, in the absence of federal data privacy legislation currently, California has the opportunity to set an example. And it is my request this law not be watered down and cannot be weakened. With the California's (inaudible) population and fifth largest economy in the world, we have the chance to set an example. Others are going to follow that. So we weaken that law, we reduce those consumer rights. That would be the example they follow.

SPEAKER TEN: My name is Mary Stone Ross (phonetic). I was one of the original proponents of the initiative that became the CCPA, and formally president of California (inaudible) I am no longer part of that group, however, my comments today are my own.

I'm here to today to remind Attorney General Becerra and his office of our original intent in firing the initiative: To give all Californian's meaningful transparency into (inaudible) personal information.
businesses are selecting about them in their devices. And unlike current privacy laws, be sure that the law be enforced.

As you are aware, the right to privacy is a fundamental right protected by the California Constitution. And the state has an interest in protecting the privacy rights of its citizens.

Today businesses can state their policies in vague terms, change them more or less at will, and offer very little, if any, privacy protection to consumers. The CCPA will change this. A shift the balance of (inaudible) towards consumer. But there are ways that your office made the protection even stronger.

Transparency. The right to know what CCPA is the cornerstone of the higher law. A consumer can only believe (inaudible) collection and sale of personal information if they understand what information is being collected. For example, if a flashlight ap (inaudible) location, that information must be disclosed up front. (inaudible) the burden on consumers to make a verifiable request (inaudible).

And even if there two standards of verifiable requests. One, is the consumer is only requesting the (inaudible) worries of the information of business
collecting. And second higher standard as a consumer is requesting the specific pieces of personal information. It should be as easy as possible for a consumer to request in categories (inaudible). It should also be legally clear a consumer can exercise the right to know categories of personal information (inaudible) specific (inaudible).

From a consumer privacy standpoint, it does make sense to have a much higher standard of verifiable request if a consumer is requesting (inaudible) of personal information. Many businesses that do not have a direct relationship with consumer still collect the consumer's personal information, the consumer should be allowed to offer a third party, including a non-profit or another business to opt out of the sale of their personal information on -- definition is critical.

I agree with some of the criticisms of the CCPA that "household" is a vague and undefined term. However, it is necessary that consumers be allowed to find out what personal information a business collects about your devices. Things, for example, my cell phone and watch travel with me everywhere. And from a data collection standpoint are essentially leading. I advise the definition of personal information is changed (inaudible) household and go back to the
original records of individuals who (inaudible).

We wanted to create a living law and the updated technology has changed. The lack of which (inaudible) past regulations. There is, therefore, a thoughtful burden on the AG's office to continuously add to categories of personal information. For starters, I would advise (inaudible) information is added back into the categories of personal information as defined by the initiative. As evidenced by (inaudible) there's clearly -- just as clearly a category that consumers condone.

Enforcement is key. I agree with concerns raised by your office, the Attorney General alone is not in the position to be the sole enforcer of (inaudible) acts. I encourage your office to work with Sacramento to allow, like the original initiative, enforcement by any district attorney or by any county counsel, city attorney or city prosecutor whose city or county meets certain population thresholds. (inaudible) non-discrimination provision is a mess and effect is non-discrimination provisions.

I encourage your office to work with Sacramento and come up with guidelines on when a consumer can sell their personal information. The understanding of privacy is not a commodity that only
the wealthy should be able to afford. Consumers are in a position of relative, and with some respect, the technologies and (inaudible) we use. Businesses have considerable expertise (inaudible) about the value (inaudible) data. Therefore, in order for the consumer to give meaningful consent, the business should have the burden to clearly define the value provided to the business by the consumer data.

Finally, I want to remind all interested parties that privacy is good for business. When we drafted the initiative, we wanted to encourage businesses to comply. One of the reasons why we decided not to regulate the reflection of personal information as this, too, is a way for consumers. I urge you to make your guidelines as clear as possible to ease the burden of the mind. Thank you.

SPEAKER 11: Hi everyone. I'm here (inaudible) I'm also a long-time (inaudible) privacy management and (inaudible).

My understanding about how (inaudible) regulated industry (inaudible) how (inaudible) works, (inaudible). So for example, the CCPA counsel (inaudible) sale of data.

What you should know is that most people in most companies (inaudible) trading to the other
(inaudible), they're exchanging it, they are providing it for the sake of (inaudible). And as you know, (inaudible) CCPA (inaudible) from the sale. So I don't think the CCPA as we know it today is going to have much impact on the (inaudible) industry, they don't think the consumers have that much choice (inaudible). So I will simply just want to encourage you to understand how that works (inaudible) for more than happy to (inaudible).

SPEAKER 12: Hello. Thank you for the opportunity to speak. (inaudible) My name is John Lewis (phonetic), (inaudible) before computers and finding people who don't want to be found, which is a (inaudible). Basically, we work with different financial institutions to help them be compliant in ways to be able to help consumers.

When a consumer gets scared, they go in hiding. They don't want to talk to people. The only way to help them is to reach them and get in touch with them, offer solutions you have to financial substitutions. Part that process is (inaudible). They're not answering their phone or returning calls, then typically what you're doing is you're gathering data on them from other data providers to try to be able to say, maybe they moved and didn't tell me and
there's a new phone number for them that I go back
somebody else has, they can help me get in touch with
them. That's the process that (inaudible).

I think the intent of the law is great. I
think it's well intended. I think it's smart, and I
think it's a law that's needed to improve some of the
manual processes that are in place right now. But
frankly, I know this because I was there when we used
to use phone books and microfiche and criss-cross with
books to gather data on, find people right of the
courthouse. That was how you gathered information by
people. Now you push a button and you got more data
than drinking water through a fire hose. There's so
much data available that it's overwhelming. And it's a
broken process how it's gathered. And I think that
there are opportunities with technology standpoint, and
I know that, I spent the last 12 years doing it, there
are opportunities from a technology standpoint to be
able to put a process in place we can add structure to
unstructured data.

Specifically, debt collection. Specifically,
from skip tracing and add structure in regard how
companies can gather, organize and track all this data
in a more organized matter. So somebody asked me what
data do you have on me, I push a button, here it is.
(inaudible), here it is. You want to delete it? No problem. Maybe you don't want to delete it because you need it because you have to keep it because in case there is some type of a reason you need that data to show why you used it to say respectfully, I used this data to never call you back, here's the data, I have it, it's safe, it's secure. That's the way that needs to be done, and that's not the way it's currently done in our industry.

So when I saw this law, I thought this law was phenomenal. I think there's opportunity (inaudible) complex, complicated. Because there's so many different systems and so many different ways to (inaudible) around. It's like the wild, wild west. Frankly, it's a little scary.

I think this is an opportunity for stronger guidelines (inaudible) how the data is housed, after it's sold or shared to ensure the data is always held a security platform that we see in industry standards. As you said today, there's industry standards, (inaudible) guidelines, you just want to know the rules are. The rules need to be clarified to understand, hey, this law is great, but I need time to be able to do it (inaudible) does what meaning everything you're touching right now is in play starting January 1st,
2020? Those are the questions we need answered.

We're also hoping that the law makers specifically can clarify, for our industry anyway, GOP exemption. I just went a two-week tour with some of the biggest banks in the country, and a lot of them haven't even heard of this law, let alone understand really what the implications are, what it means.

So for example, if a California consumer asked a banker or vendor of the bank what data they have on them, the bank or the vendor need to share what data they gathered on the customer there, or the example having to disclose this information, also.

And there's clarification that's also needed in the outbound language, how can the CCPA apply data gathered on consumers who are not the bank? We're looking to somebody, you may pull a report on thousands other California consumers on that report. It's all trackable if you're using a system that can track it. But the question is, is this law in play when it applies to that?

So I think that's just a lot of opportunity (inaudible) people in the weeks to understand data and to understand what's happening to be able to give you guys the clarification how a widespread and far-reaching law like this can actually be used for the
benefit of what we all want anyway, which is our own
data privacy. Thank you again. Appreciate the effort.

SPEAKER 13: Hi everyone. My name is Tracy
(inaudible). We're a Northern California democratic
communication.

I just want to know because this is the
second CCPA forum that I attended. Compared to the
first one in San Francisco, I just want to sort of
compliment you, this room, in terms of it being far
more diverse crowd, far more well-thought out
perspective. As this process is moving on, I think we
are seeing some improvements, which are good to see.

I'm not going to completely reiterate the
comments that I made in San Francisco, but that would
be boring, A, you already have them. And I (inaudible)

I do want to sort of reiterate with all of
the people that are here, with the improvement in
diversity, there's still somewhat absent or missing the
public, the consumers, what I would call the unrelated
parties that don't handle data for a living, that are
in privacy professional, but they're simply on the user
side of the (inaudible) I haven't seen too many
comments here from those folks. So to an extent, I'm
going to try to channel some of that because I think
it's really, really important that this law work for
the people that are on the users side, and not (inaudible) or the businesses that would be regulated by it, although that is also important. But it can't be sorted a one-sided conversation where essentially the nature of the regulation (inaudible) filled out by others who are being regulated by it, because we have seen (inaudible).

So in terms of sort of consumers, I think whatever gives people a right, it's important that there not be any penalties inherent or connected with that right. We give people the right to vote. We don't want it to be accompanied (inaudible) or the idea if you show up, someone is going (inaudible) in the head, which of course has happened.

So when we're giving people the right to opt out, that right should be as free and as unfettered as possible. So when they look at what my colleagues describe as the non-discrimination (inaudible) in the current version of CCPA, what we see is that I could pay a less (inaudible), we see that I could (inaudible) or a service could be (inaudible) in some way. (inaudible) should value my data which is a squishy term what we're not entirely sure what it means. But essentially there is, you know, there's potentially a price for the exercising of the right (inaudible). And
of course, I may chose to exercise the right with one company that breaks me out, or I may make a decision to implement it over and over and over again, any number of companies that I think (inaudible) impacted by. And accumulated (inaudible) over and over and over again is what we would call potentially a chilling (inaudible).

I think it's important that you sort of take a look how is this law going to sort of land on the heads of the people that it is supposed to be helping. Because there is much of a safe holder as all of the companies that are here.

SPEAKER 14: Good afternoon. Grand (inaudible) from Dallas, Texas. And I work for a large company here today and consult business on the side.

What's relevant to that why I bring that up there are several companies relocating to North Texas, as well as Texas (inaudible). As part of their (inaudible) a lot of their employees are retreating to rent in Texas to stay, just (inaudible). So what's happening is a lot of small businesses in states like Texas are now basically availing themselves (inaudible) rules they have to follow. The problem is in Texas, what we consider as reasonable security and people's privacy is quite different than what reasonable privacy, reasonable security in Texas.
So (inaudible), you have to understand what exactly is reasonable security with respect to CCPA (inaudible) in California versus those in other states. I believe (inaudible) commerce because as you know, today there are now is letting commerce (inaudible) United States in the world. And also, those moving to Texas (inaudible). So (inaudible) adopting this, provide clear guidance, if you will, to what is considered reasonable security and reasonable privacy practices. That would be a great and beneficial to all of us having (inaudible). Thank you.

SPEAKER 15: My name is (inaudible) vice chair (inaudible) consumer privacy. This is the organization that all by the initiative, the Consumer Privacy Act with over 700,000 signatures and telephone which lead to the Legislature passing what we see, are discussing here today.

As a co-author of the CCPA, one of the (inaudible) comments on these two areas (inaudible) verification on consumer request, will certainly verification and consumer request, and specifically (inaudible). And we define whole pages any page collecting info. So unless there's some confusion around that, it's our belief that we don't think the law really deviates from this as written, that it
really is any page that's collecting (inaudible) stops
the home page as defined more broadly. In the
community, it's actually (inaudible) defined that
actually collects information.

We think this is important because, again,
being able to opt out and be able to do the right to do
should be known, should be able to access it and do it.

One last thing before just (inaudible) we are
concerned about reports from Europe that large social
media companies with the relationship with the consumer
are taking steps (inaudible) allows them to be,
quote-unquote, co-first parties. When a consumer
visits a site, even though any rational consumer would
only think they were interacting with the site they
were on. So let's assume the consumer goes to a
fictitious site called Newspaper.com, and thinks it
achieves only Newspaper.com website, but actually
Search.com, another fictitious site, and
Socialmedia.com have sent cookies on Newspaper.com, and
suddenly are treating the consumer as their own
consumer. And so everything the consumer is doing on
Newspaper.com is (inaudible) Socialmedia.com. That's
clearly not the intention of GDPR from our perspective.
And we hope the Attorney General's will assure that's
not allowed under CCPA, that type of thinking.
So finally, Section 185 B is the reason why we're here today. When we crafted this law, we had the choice to make in terms of whom we thought (inaudible) regulations. We're happy we chose the Attorney General's office. We think they're in the best position to move quickly, judiciously, and all the information necessary to make these regulations as appropriate as possible.

Finally, I have just (inaudible) point. Before we cut the deal with the Legislature, we did a pole on CCPA. This is where sometime in June of last year, this thing polled at 81 percent. So since then, there has been a lot of changes in the industry that I think actually make that poll even higher. So I encourage all of you embrace CCPA, good for business, good for consumers, move forward to enhancing the rights to consumers (inaudible). Thank you very much.

SPEAKER 16: Good afternoon. My name is George (inaudible) in the state of California. (inaudible) CCPA, as well as profit of the privacy section (inaudible), I, (inaudible) security scientist (inaudible) member for some of the internet service content, who were still businessmen or law of fundamentals (inaudible).

I'm also recipient of global IP (inaudible)
pioneer award (inaudible) wireless (inaudible)
publication and internet security standards (inaudible)
generation wired and wireless internet technologies,
including the collaborative (inaudible) networks
(inaudible) Dr. Larry Roberts and Jim Valance.

I've also dedicated my life to setting
standards in technology, privacy and cyber security.
My path emerged after I lost my wife, (inaudible) to
breast cancer where I was grieving with other widowers
who had their deceased wife's privacy data stolen while
settling their estates.

Thus, I take the complications and technical
matters related to any law of data collection
(inaudible) monitoring the privacy data to heart. I
will love to (inaudible) elements for privacy
identification based on IP and geo location identifiers
(inaudible) legislation that present a masking false
positive, (inaudible) probable for consumers,
businesses, service providers and organizations in
general, required to monitor and (inaudible)
enforcement of defense of privacy (inaudible).

First, public IP addressing can be mapped or
changed (inaudible) tunnels dynamically services and
other virtual privacy methods that present enforcement
challenges for a consumer pursuing their privacy
rights, or for a business defending their privacy protection position.

We suggest that IP addressing as a unique identifier be enhanced or replaced with a different IP infrastructure (inaudible) track more accurately, as well as additional attributes uniformly shared by the IP four and IP addresses.

Secondly, we want to know that with regards to geo location and (inaudible) technology addresses used by the largest (inaudible) service providers who are (inaudible) consumer privacy data, that the noting of the technical monitoring complication the IP six to IP four (inaudible) issues, coupled with the inherit (inaudible) providing of geo location, extremely accurate today, will severely impact the geo location monitor date of making archived collection of (inaudible) accountable. We do suggest a multi-faceted enhancement of geo location identifier or eliminate (inaudible).

Consequently, these are complicated, technical challenges that may require (inaudible) and design do make current CCPA enforcement deadline (inaudible). And I do recommend that Americans, myself, the American (inaudible) numbers, California ID Task Force, the internet appropriation (inaudible) for
(inaudible) numbers and provide (inaudible) and all my comments due to their technicalities will be published in an e-mail address. Thank you.

SPEAKER 17: Hello. My name is Andrew Lackman (phonetic). I'm an attorney who works in data privacy. Most of my clients have less than 25 employees. So probably just by virtue of revenue alone, probably don't fall under this legislation, although with the 50,000 records, it's always possible.

I also was the legislative director for Congressman (inaudible), which is a graduate of this prestigious institution, and attended Stanford undergrad.

And I made this meeting here today. I wanted to make Sacramento, but Delta decided it didn't have a plane. There's some things you can't control.

But in attending the recent hearings out of Sacramento on the bill itself, it became clear there's another issue which hasn't fully been addressed in all of this. And I do want to go right now, as we speak, they're holding hearings on the exact same issue in Sacramento. I don't know who decided to have two meetings on the same issue at the same time, but I think it does a disservice to many of the people here who maybe care about changes to the legislation who
can't afford to have staff in multiple places. I work for myself, and until I figure out the cloning policy, I can only be in one place at one time.

But the issue that did come up was within the definition of what is personal information. And the definition in the legislation says, it's any information which can be ascribed to an individual. But, many companies either consciously pair or unpair information so that any piece of information you can collection be ascribed to an individual, if you give the other information. And so because of the broad definition, it creates about what is and isn't.

However, within GDPR, they have actually addressed this by requiring companies through data mapping to show what information they don't pair. And so having that information, you can say, hey, I maybe I collect an e-mail address and phone number of somebody, but I don't pair that or connect that with their purchase history, and here is how I separate it out. And so by giving companies the opportunity to document and prove that they do not pair this information, that should be a reasonable alternative to make sure that instead, they're not required to provide every piece of information that they possibly could pair conceding in the universe, if it's possible to do so.
So I'm going to be take to heart suggestions about writing specific regulations, and I will be providing those before the deadline. But did want to bring that up as a very particular problem which can be addressed within the regulatory context, which won't change the (inaudible), and allows companies of all sizes to be able to comply with the needs of the public, while at the same time, not having to double, triple or quadruple staffs to deal with potential data subjects request. Thank you very much.

SPEAKER 18: Hello. My name is (inaudible) I work for (inaudible) running business (audible).

Couple things became very one (inaudible) request because, for example, in the average world data (inaudible). Every time you go to a web page you see an ap. In order to facilitate that ap, (inaudible) that share your data with consumer (inaudible) about web pages see data has been shared with some of the website. I think data was important, (inaudible) problems that to be able to make four, five companies that (inaudible) and wouldn't be able to (inaudible) consumers to data know.

And basically, (inaudible) from consumers in Europe and (inaudible) consumers (inaudible) some kind of (inaudible) enough to (inaudible) what do you do
about those (inaudible) I think I'm making the point
(inaudible).

For example, (inaudible). Quick comment
(inaudible) comment would be for the (inaudible) and my
education thought (inaudible) because many IP apply to
account for online they don't need my ID my account
they need my ID to get my account. Example I signed up
for (inaudible) and then put my account on hold because
they respected (inaudible) have and then I said
(inaudible) IT to get my and sign me up for their
e-mails, and I don't want to receive the e-mails. So
my e-mail list from your mailing list and they want my
ID (inaudible). So whatever phone number (inaudible)
using my for example so if I want to have (inaudible),
they don't need my ID because I gave them my ID the
first day. (inaudible).

SPEAKER 19: Can you hear me? My name is
(inaudible). I'm speaking of the private, retired and
legally disabled citizen. And I sense a gap in
(inaudible) law so have cross the law step out and stay
(inaudible) to charge me money to protect my privacy,
which offer me incentives so I'll surrender my personal
information (inaudible) act and this coercion.

California, as well as most of US, it's
illegal for an employer to discriminate or harass an
employee over 40 years of age or older (inaudible) and a class. And state laws of California Fair Employment, Housing, familiar with Section 1798.185 and I spend a lot of time trying to find it (inaudible) are now something I might have to pay for. And that's new and (inaudible). How does that work? I couldn't find an answer.

So because the a lot of us retired, on fixed incomes, we have to choose between rent, utility, telephone bills, transportation, clothing or protect our privacy, which (inaudible).

And cutting to the chase, if you look up the definition of "coercion," it's asking you to do something you don't want to do. And it's 1798.125 P four, coercion. So I think that something has to be taken into account for people like me (inaudible) to privacy violation in general (inaudible) legislation. Thank you.

SPEAKER 20: Thanks. My name is Allen (inaudible). I'm an attorney licensed in New York, certified information (inaudible) privacy (inaudible) professionals. I have a legal consulting practice that works primarily with advertising technology and marketing technology. So please (inaudible) in response for your request. And I appreciate the
opportunity to.

I believe it will be difficult for ad tech and (inaudible) businesses to implement CCPA without some additional clarification. And these (inaudible) challenges are particularly noteworthy given what I can see was going on in Sacramento that there maybe a push towards ensuring a private right of action under CCPA. That has become (inaudible) issues to grave concerns to the extent that there is a huge lack of clarity (inaudible).

So first, it is unclear whether ad tech companies are considered third parties or service providers under the CCPA. I think even today you see one person stand and say, oh, no. They're all service providers, and somebody else say, no, they're in fact third parties. So that, to me, would be inhibit us that reasonable people can and are disagreeing about those particular definitions.

And this distinction is particularly important in the transfers of data to third parties in business considered of sale on (inaudible) and therefore, subject to (inaudible) choice requirements.

So specifically, the CCPA requires notice of choice each time data is transferred that Section 1798 over 100 stipulates that the notice provided must be,
quote, at or before the point of collection, unquote.

So, if ad tech companies adopt a conservative view (inaudible) third parties, that means that a separate notice is in choice must be offered each time data is transferred. So bringing this requirement into the ad tech world, I'm just going to apologize in advance for a little bit into the weeds here, but when a website publisher transfers data to an advertising exchange (inaudible) provided. And when that ad exchange provides data to an ad server or demand site platform, a separate notice and choice must be provided. And with the demand site platform transfer data, (inaudible) ad verification partner. An additional notice of choice is required. And when the demand site platform transfers data to a data management platform -- okay, I think you understand where I'm coming from.

So a single act in this example would necessitate the provision of notice and choice four separate times. That's assuming there's only one ad on a single web page. Most web publishers have three, four, five, ten. So the four time number goes up exponentially. And if you want to honor the literal requirement of the CCPA, you would need to have something like 20 separate notice and choice
(inaudible) being launched on a consumer. And don't think that would be the intent, and I don't think that anybody wants that. But that's a reasonable read of how the act is currently being -- as it currently reads.

Okay. So I believe there are a few clarifications that may address this issue. Number one, please clarify what an NTP (inaudible) is a service provider versus third party.

Number two, clarify what constitutes a business purposes under CCPA. Again, I read that definition to mean that just about anything an ad tech or mar tech company does would be considered business (inaudible). But I have colleagues whom I respect greatly who take a different position. We would like clarification on that.

And number three, clarify the sales of data passed near real time would only necessitate the provision of a single notice and choice. I think that's the intent of the legislature, but it isn't how the law currently reads.

My second point, a digital media space would benefit with some clarification providing a choice (inaudible). So that CCPA requires businesses to post a "do not sell my data" on the website. I would concur
with my colleague, Rich -- actually, we're not really colleagues (inaudible). But the gentleman in his comments, in that I do think (inaudible) goes on every single web page. But so I think I understand the intent, but without some clarification, this "do not sell" button would be difficult to implement in part, because those requirements is currently worded (inaudible).

Just by way of quick background, the way digital media opt out currently work is they are vendor specific. So it is an ad tech vendor that the consumer has to be capability of opting out from. CCPA places those requirements on businesses and third parties. So the requirement would be an advertising publisher would enable opt out from then. So that's not how the part opt out situation is set up. And I think we just need a little bit of clarification regarding whether or not the industry opt out pages (inaudible). We need some clarification whether those are sufficient under the AG's interpretation of the CCPA.

I know over time, I apologize, but thank you very much. I appreciate it.

SPEAKER 21: I'll go quickly, and I (inaudible).

Quick overview. You heard some people
transfer data to another person to another person to
another person. (inaudible) six different
subprocessors for (inaudible) without any of the
indication or awareness being made to the consumer,
without them being in the same country, the same
network, or even the same universe.

So in reality, we need a mechanism, which I
don't currently see (inaudible) I'm limiting what you
can do, there we will need to have (inaudible)
controller, processor, which is the definition of the
rest of the world (inaudible) other laws.

With regard to the questions asked, I will
make a few requests. Request number one, please make
sure that the law requires the assignment of the data
protection officer, whether that is his or her
(inaudible). Right now, the responsibility in the
organization is not that clear.

Second request, the definition of "personal
information", we should clarify, we should make it
probably similar in the (inaudible) we should also
create a higher level of SPI and clarify the approach
to PHI (inaudible)

Next point, without transparency, there
cannot be any formed consent. The point of
transparency has got to their own, if we are to say a
person owns their data and can control what we share.

Next request, we are requesting that the ID of electronic devices will be completely forbidden for businesses polling, except for in the case of law enforcement requirements.

Next request, verification. The GDPR makes it clear that the verification of the individual's request in the subject access request should not be more onerous than the creation of the record in the first place. In other words, if you trust who I am by asking first name and last name, please accept my request when I provide you only my last name and first name -- okay.

We are requesting clarification regarding the conflict of HIPAA and regarding GOPS. Well, and we are also asking for clarification regarding the US Constitution Congress clause. In other words, some of my clients are going to come to rely on the CCPA, and it will be very sad because Congress calls the situation where their compliance is completely nullified.

We're requesting clarification of the (inaudible). When somebody's GPS is tracking, what happens when they enter the State of California? What rights or obligations occur? (inaudible) as request
clarification of third party service providers, data
brokers, and of selling.

I read this law quite a few times, and I
can't tell if (inaudible) first category, second
category (inaudible).

We're requesting that the disclosure of
(inaudible) right and assume data regarding individual
be included both in disclosing what (inaudible) and in
the right to object.

We mentioned, for example, the company called
(inaudible). They have a lot of data on people,
(inaudible), but the right them assume they are
(inaudible) for me, there's no rest.

We are requesting that you consider
compliance and singularization of ISO 29100 regarding
definition for personal information and the ways to
preserve personal information.

We are suggesting that the appointment of
advisory panel to advise the Attorney General and
separately other organizations within the state
regarding the interpretation and the enforcement of the
CCPA and the right (inaudible).

We are requesting clarification of the
private right to action. For two reasons. Number one,
I cannot tell my clients if they're going to be on the
hoop for $7,500 or for $7,500 per record.

Removal of the incentives with regard to how long companies collect and keep your personal data typically (inaudible) hurt the weakest (inaudible) of society, the buyer or people without means.

And finally we're asking that -- sorry. We are asking that the new (inaudible) regarding the impermissibility of sharing of data, which certain regimes or certain companies within the geography of certain regimes (inaudible) privacy.

Thank you very much.

SPEAKER 22: (inaudible) I have a pure observation about we have tech oil (inaudible) people to use it. (inaudible) this law is very broad. And what I would like us to kind of understand is that if we have nothing to protect consumers today, we should find a reliable product of protection rather than (inaudible) for businesses to be able to verify and produce a verifiable solution, easily accessed and be able to understand. And because businesses will be able to comply. What is (inaudible) in this law?

Number two, the AG's office has to come up with a way to audit businesses are complying to this. The point is that compliance (inaudible).

So going into one of the sections of 1798.135
C, consumer may authorize another person to be able to request on their behalf, how do we communicate with this person? What is the authorization (inaudible) Secretary of State who somebody actually authorized this. (inaudible) communication electronic? It's communication is (inaudible) web page where consumer comes in who doesn't probably (inaudible) have an account. (inaudible) collect information to be able to see whether they exist in the system, how long are we allowed to keep the records so we know that verifiable request, if that information happens to be first name, last name, (inaudible) all because that is how verify in the system that the person's name exists? How are we supposed to retain if it is going to be twice in a year? If you request it already once or twice, we can keep (inaudible) at some point, we're going to have to tell the consumer, hey, you already (inaudible) two limit, or we have to maintain a record another (inaudible) trace, a verification on communication. So there's a lot of things that needs to be maintained in a system that could require if you have an account tying to your ID as a consumer who is registered business, which you do not have it, but a consumer keeps coming every month just to test it, how do we keep track of that consumer coming in? Right.
So there are a lot of these questions that are (inaudible) asking for ID verification. Well, there's pros and cons to it. If you want to protect the consumer, you have to identify it is who you're requesting is actually a consumer or an authorized person. Obviously, it's easy to create an account because that is what we allow people to create an account. If somebody wants to destroy something, you verify. It's everywhere.

It's ease to see how this is going to be somewhat managed in a way that is going to make both consumer and the businesses to be able to work together in a simple (inaudible).

SPEAKER 23: Good afternoon. My name is (inaudible) I'm an attorney and from Texas. And I want to first and foremost tell you that I wanted (inaudible) people said --

MS. KIM: Could you speak a little closer to the mike.

SPEAKER 23: (inaudible) I agree. The CCPA is not perfect. It isn't. Yet, how it's written, and more importantly, interpreted bear on how the issues position regulations on something and (inaudible) I spent 17 years in my career (inaudible).

First one is balance. Respectfully disagree
with some of the people here today. Balance must be made between (inaudible).

Reasonable regulations. What you are dealing with is imperfect law and (inaudible). California is a fifth largest economy (inaudible). I urge you to concentrate on clarity all for parties involved compliance for (inaudible) exercising consumer rights. Narrow definition in particular sale and business (inaudible) consequences in abuse, establish regulations that have compliance which you need. (inaudible) and one, that is the definition, which you also (inaudible).

Respectfully, amendments (inaudible). One thing I must say as an example when correction in conflict in particular time period with which (inaudible) has to respond. (inaudible) formerly mentioned (inaudible) that's not the only constitutional issue here.

Obviously, any comments to assist you (inaudible). Thank you for your time.

SPEAKER 25: (inaudible) my comments, my name is Heidi. I have a broad set of personal experiences that (inaudible) my comments. I'm a mom, I care very deeply about my kids' privacy, and in the amount of time they spend on their aps, and how that reflects on
me as a parent. Too much. But I do worry about them having the permanent record of their behaviors online. So I really wanted to applaud the sections of the CCPA that apply to children's privacy.

I worked in tech for over a decade. I worked in the data protection space (inaudible). My experience there was that if there's no threat of enforcement, there is no business justification to make any expensive changes to the way that companies operates. The way that the businesses analyzed (inaudible) a risk analysis. And what goes into it is what'd the impact, you know, how much of a fine potentially is there going to be to my business, and what's likelihood that the Attorney General or the -- any other enforcement agency is really going to do anything?

So I just think it's (inaudible) so critical. And we know currently in the state Senate and (inaudible) the Attorney General's office (inaudible) Legislature, there is few people who are talking about local government enforcement (inaudible) common sense media. And I think the Attorney General will be allies.

And I would like to encourage you to consider local counties and city attorneys as an extended force
that you can call upon. I think the law does give you
the authority to act broadly in that way and put that
stipulation into the law, assuming that the Legislature
does not do that -- they're not currently doing that.

In fact, at the state assembly hearing,
Assembly Member Irwin is actually confused about
whether that still exists in the law or not.

So with our legislative (inaudible) I think
it's up to you (inaudible) to act (inaudible) if we
really want to see change with the way our personal
data is being handled by the companies.

And the economy in this area is growing so
fast largely because (inaudible) probably more than
half my close friends work for those companies. I
don't want to see damage done to the economy and to my
friends' industries, however, it's just gotten out of
control. And I think the balance currently has shifted
way in favor of business to the point it really
threatens democracy as we know it. It's (inaudible)
and enforcement actions. Someone who's worked in tech
for many years, and someone who currently works in a
local government, which I will remain anonymous about,
because we are providing formal comments, written
(inaudible).

So I don't envy your job. Good luck to you.
And thank you for letting me comment.

MS. KIM: After this comment, we'll take a short break and then we'll resume.

SPEAKER 26: My name is Joellen Kaiser (phonetic), and I came here today to comment.

I'm on the board of a non-profit as concerned about privacy. But I'm actually speaking you to today as an ordinary citizen. Because as I'm listening to the comments, I realize that there's a population that is almost never considered in this kind of rule making that really needs to be thought about, especially when we're talking about categories and who gets to make decisions about somebody's information, whether it's an individual or household.

I'm a caregiver for two elderly relatives. And these are people who, guardianship is a really huge step to take with elderly relatives. You don't want to go into guardianship and go into courts if you don't have to. It hurts their sense of dignity. Some (inaudible) powers of attorney around finance and health care.

But what we find is, increasingly, we have to do things online for them. Things such as managing their newspaper subscriptions. Everything is online. And we have to get lists for them to go places
(inaudible). You know what I mean? It's all online.

And I'm starting to say, I'm starting to realize that I'm in situation of such seniors. In fact, any of us who suddenly become ill and unable to get on our computer, how do we verify the person who is going be able to act on their behalf?

And what if it's not a relative? What if they're not in a household? I have friends who take care of elderly, single people, and they're not their relatives. They're their close friends.

So what is going to be the mechanism of what would power of attorney serve in that place? What (inaudible) going to help us understand who would be in charge of some of this information?

And it's really -- especially with seniors, they're very freaked out about personal information in a way I think most of us have given up on in some ways. Seniors are really upset about it. So I'm really asking you as in your roll making, in addition to consider kids and those of us (inaudible) please consider seniors. Thanks.

MS. KIM: Thank you guys. It is about 2:52 so we'll take a break until about 3:05 and resume if there's additional comments to be made. Thank you.

(Off the record.)
MS. KIM: Thank you so much for sticking around. We're going to go ahead and get started again. So if there are any additional speakers, please feel free to come forward to the mike, or come to the front. And if there's nobody we're going sit in silence for a little bit.

SPEAKER 27: (inaudible) personal comments (inaudible).

SPEAKER 28: I'm not trying to pretend I'm somebody else by standing on this side of the room.

I just have one additional comment I didn't get to. I don't think anybody here really brought up. You guys have a huge job. There's a lot of work that needs to happen. So what I'm understanding the timeline right now called to start the process that's provided guidance, which to me is guidance may not be received until sometime (inaudible) companies that are fairly put if you're dealing with companies like the agency holding company or General Electric or somebody who's really large, that's like turning around an aircraft carrier. And I would just respectfully say that six months is probably not going to be enough time for a lot of these types of changes to be implemented. Particularly in light of some of the perceived ambiguities.
So I recognize the AG's office -- deadline has already been extended. I would strongly encourage you to consider extending it further, particularly if the AG's office is not able to get guidance, you know, by September or so.

I appreciate the need to get this right. And so I think that's a lot of the world to support. But if the -- if we don't have guidance, you know, until three months before we're supposed to comply, that's just going to be a huge problem. Thank you.

SPEAKER 29: (inaudible) We also concerned about (inaudible) action. Because you said the Attorney General will not be prosecuting until a certain deadline. But I don't see anything saying that the deadline for privacy causes of action (inaudible) January 1. So we're looking at (inaudible) 2020 that rules people (inaudible). So with the deadlines, please don't forget that they try to (inaudible) action as well because everybody have the opportunity. Thank you.

MS. KIM: Sorry. I recognize this is a bit of an uncomfortable silence. It's something that we call air courage so that if there is anybody else who
maybe considered wanting to speak, but didn't have the
courage to do so, we'll just sit in silence for a
while.

But feel free to take a stand or just if you
would like to leave, you're welcome to. If you like to
stick around, we are probably going to stick around for
at least another 10, 15 minutes.

SPEAKER 30: I just want to make a comment.
My name is (inaudible) I'm an attorney, (inaudible) I
have thoughts on the law, based on some discussions
I've had in the (inaudible) area.

I think what we need is (inaudible) clarity.
I have four points that I would like to make.

The first is I would like to see clarity in
the definition of the term "category" (inaudible). It
would be nice to see where the AG considered categories
of businesses, how expansive they need to be in
descriptions (inaudible) disclosures.

Second, it would be nice know what makes a
request manifestly towards unfounded or excessive.
Businesses are not required to respond to request
(inaudible) excessive but that term is not defined. So
clarity in that definition would be helpful.

Finally, I think it was mentioned earlier by
the gentleman to your left, there is an contribution in
the law regarding when businesses must respond to the consumer request. So under 1798.1382, business is entitled to a (inaudible) deadline extension of the time to respond as reasonable. But under 145 (inaudible), a 90-day deadline or extension of the deadline is provided. So each of those businesses get extension (inaudible).

MS. KIM: Thank you everyone for coming. I just want to remind you that you can submit written comments to that e-mail address on the Power Point slide, or you can mail them in as well. And we strongly encourage you to do it by this Friday. Thank you.

---oOo---

REPORTER'S CERTIFICATE

---oOo---

I, SHANNON D. DENNEY, CSR 10385, a Certified Shorthand Reporter in the State of California, do hereby certify:

That the foregoing audio recording was transcribed by me; that a verbatim record of the recording was made by me using machine shorthand, which was transcribed to the best of my ability.

IN WITNESS THEREOF, I have this date subscribed my name.

Dated: April 12, 2019.

Shannon D. Denney, CSR 10385
Certified Shorthand Reporter
State of California