

MEETING OF THE
CALIFORNIA PRIVACY PROTECTION AGENCY

(Pages 1 - 133)

Location: California Public Utilities Commission
Auditorium, 505 Van Ness Avenue, San Francisco, CA
94102
Date: August 6, 2026
Transcribed by: Brandon Iorlano

1 APPEARANCES:

2
3 Jennifer M. Urban - Chairperson

4 Drew Liebert - Board Member

5 Jill Hamer - Board Member

6 Nicole Ozer - Board Member

7 Tom Kemp - Executive Director

8 Phil Laird - General Counsel

9 Lisa Kim - Senior Privacy Counsel

10 Rianna Grenda - Senior Legal Analyst

11 Sebastian Zimmeck

12 Daniel Goldberg

13 Christo Wilson

14 Stacey Schesser

15

16

17

18

19

20

21

22

23

24

25

PROCEEDINGS

CHAIR URBAN: Good afternoon. Welcome to the California Privacy Protection Agency's Informational Board Session and Board Meeting. We will be holding these over the course of today, August 6, 2026, and tomorrow, August 7, 2026.

We are meeting in San Francisco and in a hybrid format. So as you can see, three of my fellow board members are here in person along with members of the Agency staff. And Board Member Alistair Mactaggart will likely join us remotely for part of the meeting, but is not here right now. So welcome everyone. And I'm pleased to be here with everyone in person and the many of you joining us on Zoom.

Before we get started with the program, I have a few reminders. Please make sure your microphone is muted when you're not speaking. If you're here in person at the CPUC, please silence your cell phone to avoid any interruption. And importantly, please do you note that this meeting is being recorded.

CPU staff are also present in person, and we continue to offer the public the opportunity to watch and participate today -- in today's meeting

1 virtually.

2 Both days of the -- this meeting of the
3 Board will follow the Bagley-Keene Open Meeting Act
4 as required by law. All of the agenda and all
5 supporting materials are available here in San
6 Francisco and also on the CPPA website. You may
7 notice board members accessing devices such as
8 laptops or tablets or other devices during the
9 meeting. They are using these devices solely to
10 access board meeting materials.

11 The Board welcomes public comment, and I
12 will call for it this afternoon at the end of our
13 informational program and after other agenda items as
14 we move through the agenda later today and tomorrow.

15 Please do note the general rules for
16 public comment. Each speaker will have up to three
17 minutes to make their comments. Under the Bagley-Keene
18 Open Meeting Act, both board members and members of
19 the public may only discuss items that are listed on
20 the agenda. And for this afternoon's program, that
21 means that public comment should relate to the topics
22 discussed in the program and be limited to the topic
23 on which I have called for public comment. Members
24 of the public will have the opportunity to comment
25 either in person or via Zoom. I will provide more

1 detail about participation when we reach the time for
2 public comments at the end of the speaker program
3 today.

4 Please note that the hybrid format does
5 create some technical complexities. And please bear
6 with us if we experience any technical issues. If we
7 do, we will pause the meeting to address them as
8 needed. If you're attending remotely and you
9 experience an issue like the audio dropping, please
10 let us know by emailing us at info@CPPA.CA.gov. That
11 is India, November, Foxtrot, Oscar, at CPPA, for
12 California Privacy Protection Agency, dot CA, dot
13 gov. That inbox will be monitored throughout the
14 meeting, and we will address any technical issues
15 that arise. We will pause the meeting if it is
16 affecting the Zoom participation.

17 We'll take breaks as needed. I will
18 though be moving things along, as we have a very rich
19 program today. My many thanks to the Board members
20 for their service and everyone helping to make
21 today's meeting possible. My special thanks to
22 Executive Director Tom Kemp and Phillip Laird, our
23 general counsel, who are serving in their capacities
24 with us today, and to all of our speakers who will be
25 providing this with -- edifying information at our

1 informational session.

2 Again, we are at the California public
3 utilities commission in San Francisco, and we greatly
4 appreciate the CPC team for their hospitality and not
5 only allowing us to use their auditorium, but
6 providing assistance -- technical assistance with the
7 AV system today.

8 I'd like to thank and welcome our
9 moderator, Ms. Serena Carwile, and ask her to please
10 conduct the roll call.

11 MS. CARWILE: Board Member Hamer?

12 MS. HAMER: Present.

13 MS. CARWILE: Board Member Liebert?

14 MR. LIEBERT: Present.

15 MS. CARWILE: Board Member Mactaggart?

16 Board Member Ozer?

17 MS. OZER: Present.

18 MS. CARWILE: Chair Urban?

19 CHAIR URBAN: Present.

20 MS. CARWILE: Madam Chair, we have four
21 present and one absent board member.

22 CHAIR URBAN: Thank you, Ms. Carwile.
23 The Board has established a quorum.

24 Before we begin the substance of today's
25 meeting, I'll take a moment to explain the format for

1 the informational session. The objective of this
2 format is to allow the Board and the public to learn
3 about topics that are relevant to the Agency's work.
4 This afternoon's informational session is an overview
5 of the history, laws, and technology between opt-out
6 preference signals.

7 I want to emphasize that the views
8 expressed by our guest speakers are their own. They
9 should not be taken as the views of the Agency or the
10 Board. And I will introduce each speaker with a
11 brief biography before their presentation. Speaker
12 biographies and any slides are posted on our website
13 and are also available here in San Francisco at the
14 back of the room.

15 We'll give approximately 20 minutes for
16 each speaker and take about ten minutes for the Board
17 to ask questions. Once we've moved through all four
18 speakers, I will also open it up for public comment.
19 And just so you know, some of the east coast speakers
20 may not be able to stay the whole time, so please be
21 aware of that. We will now proceed to the first
22 informational session of the day.

23 Our first presenter is Sebastian Zimmeck,
24 who's an Associate Professor of Computer Science at
25 Wesleyan University. And he'll be speaking on the

1 background and development of the Global Privacy
2 Control. Dr. Zimmeck is an Associate Professor of
3 Computer Science, in where he directs the privacy
4 tech lab. His research focuses on the intersection
5 of information privacy, security, and law, leveraging
6 AI and program analysis techniques to bridge the gap
7 between system behavior and legal requirements.

8 He's a cofounder of the Global Privacy
9 Control of Web standard, and Dr. Zimmeck leads the
10 technical alignment efforts, assuring that software
11 systems are structurally compliant with applicable
12 laws. He holds a PhD and an MS in Computer Science
13 from Columbia University and a JD and PhD in Law from
14 the University of Kiel in Germany. His perspective
15 is informed by his background as a former attorney at
16 Fresh Field and a Google research fellow at the
17 Berkeley Center for Law and Technology. Dr. Zimmeck
18 advises government regulators and technology
19 companies.

20 Welcome, Dr. Zimmeck, and I will turn
21 things over to you.

22 DR. ZIMMECK: Yeah. Thank you so much
23 for the invitation. It's a pleasure to be here. And
24 I have prepared some slides, so I will share my
25 screen. And then I will talk for about 20 minutes,

1 and then there should be a ten-minutes Q and A. So
2 let's get started. Okay.

3 So I'll be talking about the background
4 and development of Global Privacy Control, what it
5 is, how it works, how it has evolved.

6 And, you know, to start out, okay, we
7 have a problem with opting out. And, you know, one
8 of the things that actually helped us tackle this
9 problem is the California Consumer Privacy Protection
10 Act. And, you know, here, you see some of, you know,
11 the different banners that people, you know, saw over
12 the last couple of years and are still seeing. So
13 here, you see, you know, as a user, I need to look at
14 the GDPR, US state law, Switzerland. I see here a
15 privacy notice with 1,255 technology partners to
16 share my data with. And this is just too much.

17 So we want to have a simpler way of
18 exercising your right to opt-out under the CCPA. And
19 the Global Privacy Control is that simpler way. It
20 is the mechanism so that people can exercise their
21 opt-out right under the CCPA. Imagine it as a little
22 robot that is, you know, automatically pushing the
23 opt-out button when you visit a website. So instead
24 of clicking a link or clicking a banner, you just
25 visit the website you have. Before you do that, set

1 your browser to send a GPC signal, and then that
2 happens automatically. You can opt-out for all sites
3 or just some.

4 This is also not only for websites, but
5 also for mobile ads, for IOT, basically for every
6 system where the web is the underlying communication
7 platform. So the mobile ads that you see, that you
8 use, also have ads, and those are also web based.
9 And so people should also be able to opt-out on
10 mobile ads.

11 Now, maybe some of you will think, "Well,
12 wait a minute. Don't browsers have 'do not track'
13 already?" And so what I'm showing here is a
14 screenshot of the latest Google Chrome. And it's
15 very small at the bottom, there is actually sent a
16 "do not track" request. And so we have this new
17 signal that I just mentioned, Global Privacy Control.
18 And then we have still this "do not track" setting.

19 So what's the difference? The difference
20 is that "do not track" was based on an older law.
21 It's called the California Online Privacy Protection
22 Act. And if you look here under number five, the
23 third paragraph, it requires to disclose how the
24 operator responds to web browsers' "do not track"
25 signals. I say it again. It says, "disclose how the

1 operator responds." So it actually does not say that
2 you have to comply. You just have to disclose what
3 you do. And that's a pretty dramatic difference to
4 the CCPA that actually requires compliance. And so
5 that's the difference to "do not track."

6 And so in 2020, with my collaborators, I
7 started working on Global Privacy Control. And
8 that's also a standard at the World Wide Web
9 Consortium. Or more specifically, it is a draft
10 standard. It's not yet finalized, but, you know,
11 we're on good -- we're making good progress there.
12 And it is also supported by the National Science
13 Foundation. And coincidentally, I can say just
14 yesterday, I received, you know, the official
15 approval that the National Science Foundation will
16 continue to support GPC until 2030. So we have a new
17 grant, and I'm happy to, you know, continue this
18 work.

19 And as you can see here, how did it all
20 start out? It started out with the attorney general
21 tweeting that GPC is the mechanism that is required
22 to be respected for the opt-out right under the CCPA.
23 Some people at the time called it regulation by
24 tweet.

25 It is now more elaborate, this

1 regulation. So we have now the official regulations
2 here that you can find on the CPPA website. And here
3 in this section, for example, it talks specifically
4 about the opt-out preference signals. And the third
5 paragraph here, as you can see, it says, "The
6 business shall treat the opt-out preference signal as
7 a valid request to opt-out of sale/sharing submitted
8 pursuant to" this civil code section.

9 And we have seen enforcement actions.
10 Here, against Sephora for not respecting GPC signals.
11 We also have seen actions from the CPPA here just
12 earlier this year against youth sports media company,
13 PlayOn Sports, that did not respect GPC signals. And
14 so this is very good. Without enforcement, you know,
15 it wouldn't work so well. And the regulatory
16 authorities in California are really at the forefront
17 of enforcing this.

18 They often work together with two other
19 states, my home state, Connecticut, and also
20 Colorado. And we have actually also recently seen
21 many more states joining these investigative sweeps.
22 So I think we will see much more in the next month
23 and years. There is the California Consumer Privacy
24 Act, the Colorado Privacy Act, the Connecticut Data
25 Privacy Act, New Jersey Privacy Act, and the Oregon

1 Consumer Privacy Act for which it is explicit that
2 GPC is required. There may be more laws where it is
3 required, but these, definitely GPC applies.

4 And there are different approaches that
5 the states take. So in California, we have a
6 statute. We have the CCPA, and then we have
7 regulations that spell out in more detail how to
8 respect privacy preference signals.

9 In Colorado, we also have a statute and
10 regulations. And then we have a Universal Opt-Out
11 List. So that is sort of -- you know, you can apply.
12 You have a signal. And then if it satisfies the
13 requirements of the regulations, you know, it will be
14 on this opt-out list and will also be required. And
15 GPC is, at the moment, the only signal. But I
16 remember when the opt-out list came out, we actually
17 submitted also the app, you know, tracking framework
18 of Apple. We took the liberty to do it on behalf of
19 Apple, but it was not recognized at the time.

20 And then we have a Connecticut with --
21 which has a statute and then informal guidance how to
22 respect GPC. So for example, on websites of the
23 state, frequently asked questions, and so on and so
24 forth. So there are these different ways of how, you
25 know, states conveyed this information and how they

1 approached this.

2 Now, I'm talking about states here. One
3 important thing to note is that, you know, these are
4 state laws. We have local laws. We don't have a
5 federal law, and we also don't have an international
6 law. And so, what does the GPC signal mean in the
7 different, you know, geographies? And you know, the
8 answer is it means what the specific regulator says
9 it means. So we have just one setting. It will be
10 required in all browsers starting next year,
11 according to a California law, an amendment of the
12 CCPA. And this setting is the same everywhere unless
13 browser makes a specific California browser,
14 Connecticut browser, and so on and so forth, which I
15 -- but then the meaning of that signal will be
16 different depending on where people live, where are
17 the people, you know, using that browser, which law
18 applies to them. And so while we don't expect it to
19 be dramatically different in the different states in
20 the US, it can be, you know, slightly different. It
21 can have slightly different nuances.

22 I'm also working with regulators in the
23 EU. With the EU commission, for example, to bring
24 GPC to the EU. And so there, we need to do the same
25 mapping that I just said here. And so under EU law,

1 it could mean, for example, withdrawing consent for
2 behavioral advertising, plus objecting to processing
3 if the legal basis for the processing is legitimate
4 interest. There is a new effort in the EU, it's
5 called the digital omnibus, to make the EU more --
6 you know, modernize it. And so there is an article
7 that changes the GDPR that also has privacy
8 preference signals, but it's not clear whether it
9 will become law or not. And for the EU, this is also
10 about solving the cookie banner problem.

11 Now, let's talk about that for a moment.
12 Cookie banners and privacy preference signals.
13 What's the difference? Are they the same? You know,
14 what's their connection? And when I talk here about
15 cookies, I don't only mean technically HTTP cookies,
16 but I mean all the tracking mechanisms that are being
17 used, you know, for advertising. And so, you know,
18 if you look at a different, you know, website, for
19 example, what you see is here. For example, oh, your
20 browser's Global Privacy Control is enabled.
21 Nonessential cookies have been automatically
22 disabled. So this is, you know, something that I
23 have seen websites doing. And I don't have a
24 systematic study on that, but the point here is that
25 when you enable your GPC signal, then websites often

1 will at least disable targeting cookies for
2 advertising, or as in this case here, disable all
3 non-necessary cookies. And so that's the connection
4 between, you know, the privacy preference signals and
5 the cookies that -- you know, there is this overlap
6 of cookies that are used for advertising that could
7 also be a sale or sharing of personal information
8 under the CCPA. And so at a minimum, that would need
9 to be turned off. And so in that sense, it might
10 also reduce cookie banners.

11 We have some measurements. We do
12 measurements ourselves. I'm citing here also
13 something from a colleague. Enabling GPC initially
14 reduces the number of intractable cookies by 30% on
15 average, with a further 32% reduction possible on
16 subsequent visits by rejecting the banners.

17 We have adoption and various browsers and
18 browser extensions. So if you use the Brave,
19 Firefox, or DuckDuckGo browser, for example, there is
20 already in the setting of the browser a Global
21 Privacy Control setting. Also, if you use a
22 different browser, you can use a browser extension to
23 get that GPC setting. Or starting next year,
24 according to the California up -- meat act, all
25 browsers are required to have a setting for GPC. And

1 we have seen in beta versions of, for example, the
2 Apple Safari browser that there is already a GPC
3 setting in there.

4 Then for the website, they often use what
5 is called consent management platforms to receive
6 that signal. So we're also working with, you know,
7 most of these -- I think probably all of them,
8 actually. I mean, the major ones at least. And then
9 there are the sites that, you know, respect the
10 signals. Here just showing you some -- at least
11 385,000 sites at the moment respect GPC. But that's
12 lower bound. It is likely more. These are only the
13 ones that advertise it, you know, that they do it.

14 We work with privacy and consumer
15 organizations. So consumer reports, for example, is
16 a major contributor here to Global Privacy Control
17 and then also with regulators. So with yourself here
18 in California, but also with Colorado and
19 Connecticut, for example. Here, you just see some
20 sites. You can go to this website that I'm showing
21 here, and, you know, that's what I was referring to.
22 You know, these are the sites that positively
23 indicate that they respect GPC. And, you know, just
24 to say a little bit about the technicalities here.
25 So if you go, for example, to the Washington Post and

1 you go to this URL, .well-known/GPC.json, then there
2 is a file that says, we respect GPC. This is
3 according to the specification that I mentioned
4 earlier. And, you know, here is the specification.
5 We're working on that. And the idea is that we want
6 to build privacy into the structure of the web. So
7 this should not be tagged on as, you know -- and, you
8 know, optional possibility, but rather, it should be
9 inherent in the web. And that's the reason why we do
10 this specification effort at the W3C.

11 GPC works in two ways. As I said, you
12 know, I imagine this little robot that is sending the
13 signal, and that is technically an HTTP header. So
14 every time you send the request to see, for example,
15 the New York Times website, you transmit also this
16 GPC signal. The recipient does not need to keep
17 track of this because with every request that you
18 make, you receive the same signal again. And once
19 you have done that, then there is something called
20 the DOM property, which essentially, you can imagine
21 as a storage in your browser that keeps track on --
22 okay, this browser is opted out. This browser has
23 turned on GPC. And that can also be requested by
24 advertisers.

25 As a side note, many advertising networks

1 that are integrated on site prefer to get a GPC
2 signal via the DOM property because it is a little
3 bit quicker. They want to know as soon as possible,
4 can I tailor the advertising here to this user, or do
5 I show a generic or contextual ad.

6 A very small background. Again, GPC
7 integrates into the current ad ecosystem, which, you
8 know, isn't perfect. I would say, you know, it could
9 be substantially improved. But, you know, the idea
10 is the following: The GPC signal will be sent to all
11 first party websites, for example, you know, a
12 publisher like the New York Times or, you know,
13 Netflix, or something like that. And those have, for
14 ad purposes, integrated ad networks, sometimes also
15 data brokers or social networks. And then the GPC
16 signal will be transformed into, for example, the
17 IABUS privacy stream or the Google restricted data
18 processing. And that is, you know, what these third
19 parties are looking for. And then they opt-out the
20 user. There's no reason why, you know, these third
21 parties could also, you know, not listen to the GPC
22 signal directly because they receive that as well.
23 But, you know, this is one of the shortcomings of the
24 current ad ecosystem, that, you know, we have to kind
25 of translate the GPC signal into these privacy flags.

1 And that's the job of the first party websites.

2 What we see in general is that there is
3 an increasing compliance over time. So what this
4 graph is intended to show is that for California, the
5 number of noncompliance site is slightly decreasing
6 over time. That is, you know, what we're observing.
7 And that is also, you know, what we continue to
8 measure over the next couple of years. And I think
9 that's interesting for two purposes. First, to see
10 where enforcement efforts are necessary, and
11 secondly, if enforcement efforts are effective. So
12 if we measure that over time, we can answer these two
13 questions.

14 Small note on what we will also do is we
15 also measure what I call here statistical ads. And
16 so that means, for example, instead of these privacy
17 flag propagation, we also check, for example -- okay,
18 we go to a realtime website and then, you know, put
19 the shirt here in the checkout cart. And then we go
20 to a different news website and see, okay, are we
21 getting an ad for that same shirt? And if that's the
22 case, then, you know, that's the sign that we were
23 not opted out despite sending the GPC signal.

24 A few points on the future. What will
25 GPC mean in the Agentic Web? So when you use ChatGPT

1 or Google, Gemini, or some other artificial
2 intelligence, how do you opt-out there? That's the
3 question we will address in the next couple of years.
4 Ideally, we want to minimize data from the beginning.
5 So the signal propagation, oh somebody has opted out.
6 Now, I cannot use their data, but still sending the
7 signal is not good. But that's the current setup of
8 the ecosystem at the moment. But we really want this
9 data shouldn't be shared in the first place. So
10 that's -- I think what we can also make actually
11 happening in the Agentic Web.

12 The final word, keep it simple. So keep
13 it simple for people to exercise their right, but
14 also keep it simple for implementers. I talk a lot
15 with, you know, website owners, and it is often that
16 they want to be compliant. And when you contact
17 them, they say, "Well, you know, thank you. We
18 actually, you know, didn't know how to do it." And
19 -- but, you know, with GPC, we can actually, you
20 know, keep it simple. It is, you know, as one of my
21 collaborators say, just one line of code that you
22 need to implement. And so I think a big part of it
23 is keeping it simple for everyone involved.

24 Okay. That's all I have. If there are
25 any questions, I'm happy to answer those.

1 CHAIR URBAN: Thank you much -- thank you
2 very much, Dr. Zimmeck.

3 Are there questions from the Board for
4 Dr. Zimmeck? Okay. I have Board Member Ozer and
5 then Board Member Liebert. Yes. All right.

6 Please go ahead, Board Member Ozer.

7 MS. OZER: Dr. Zimmeck, I just wondered,
8 what are some of sort of the big picture questions
9 you may be thinking about in terms of GPC in the
10 Agentic Web.

11 CHAIR URBAN: I'll just double down and
12 say that was my question as well. And I'm also
13 interested in any sort of general technical
14 background you can give us to say how you're thinking
15 about that problem.

16 DR. ZIMMECK: Yeah. I would like to say
17 I'm an optimist, and that the opportunity that we
18 have in this new web is actually one where we can
19 improve privacy. And the reason I think that is
20 because if people move more and more to interacting
21 with their ChatGPT, with their Google Gemini, with,
22 you know, their other AI agent, then this AI agent
23 actually can be a privacy proxy for the people
24 browsing the web. And this agent can actually be
25 smart about not disclosing data when it's not

1 necessary. And so my hope is to develop GPC not only
2 into just a signal, but actually into a mechanism for
3 data minimization.

4 Because currently, how the ad ecosystem
5 is set up -- and that's, you know, that's because it
6 has developed organically -- is that when you
7 opt-out, you are still sending your data to third
8 parties. In many cases, it's just -- it comes with
9 an op out, you know, with a privacy preference signal
10 telling the third party to not use that data, to
11 delete it when it is incoming. And so in this new
12 world in the Agentic Web where people, you know,
13 browse the web through their agent, we actually have
14 the opportunity now that the agent says, "Well, I
15 don't actually need to disclose, you know, your email
16 address or even your cookie identifier. I can omit
17 that."

18 And on the technical way, how to make
19 that happen, the current idea that we are at the
20 moment following is that there are Agentic protocols.
21 So just like there is -- you know, I told you about
22 the GPC specification on the web, there is a protocol
23 for agents -- for AI agents. One is, for example,
24 called the model context protocol. And if we can
25 build the data minimization mechanism into this model

1 context protocol, for example, I think that would be,
2 you know, a good outcome for the people using the
3 agents.

4 CHAIR URBAN: Thank you. Did that answer
5 your question, Board Member Ozer? All right.
6 Wonderful.

7 Board Member Liebert, please go ahead.

8 MR. LIEBERT: Thank you so much. Great
9 presentation, Dr. Zimmeck. I really appreciate it
10 and absolutely love your optimism. We don't often
11 get to hear that in the privacy context, to say the
12 least. So please keep coming back and getting on the
13 phone and doing everything to keep us optimistic. It
14 seems to me that the AI agent revolution is also
15 going to completely revolutionize the whole ad
16 marketing system; right? And as part of your
17 optimism, is that based on -- ultimately, it appears
18 that it's going to be these huge AI agent companies
19 that need to be regulated on the use of our private
20 information. And does that lowering -- constricting
21 of that actually lead to a potentially easier way to
22 determine whether or not our private information is
23 being protected?

24 DR. ZIMMECK: Yeah. That's a good point.
25 So let me preface that by saying that I think we will

1 have also ads in the future. So I think, you know,
2 we already see that. So I saw from ChatGPT, from
3 open AI, as well as from Microsoft Co-pilot, that
4 they have decided they will have ads. And I'm not
5 principally against that. I think there is space for
6 ads because, yeah, this has to be financed, you know.
7 And -- but it has to be done in a privacy preserving
8 way.

9 And I think I -- what you're saying,
10 that's something I think too, that, you know, if
11 there is somehow more, let's say, concentration that
12 users browsed through these AI agents, then I think
13 that could be potentially easier to regulate, indeed.
14 Because then, yeah, at the moment, you know, it is
15 very nontransparent. You know, if you go to website,
16 as I showed you, there were -- I forgot, 1,255 --
17 what was it called -- partners or something on there;
18 right? And so that is very, you know, hard to grasp
19 environment. But I think it might be more
20 streamlined if we go through this new agentic world.
21 And so I think that that is probably true. But I
22 would also say in addition, it is also true that
23 there is an opportunity to be actually systematic
24 about it.

25 So the, the current ad ecosystem has sort

1 of evolved very, let's say, positively, naturally.
2 But now we actually have the opportunity to regulate
3 it positively how that should work in the Agentic
4 Web. And I think that's another big opportunity.
5 Yeah, absolutely.

6 CHAIR URBAN: Thank you, Dr. Zimmeck.
7 This is Jennifer Urban. Again, I was hoping to
8 follow up on Board Member Liebert's question by
9 harking back to the observation you made about signal
10 propagation versus data flows, which we've been
11 talking about in terms of the Agentic Web. I would
12 like to hear your thoughts about the top two or three
13 things that you think we would need to do in order to
14 have consumers be able to express their preference in
15 this seamless way across different kinds of devices
16 and networks. What are we missing?

17 So in California, as you said, we have
18 the new law that is requiring an opt-out preference
19 signal to be in browsers. And so that is obviously
20 really important. Are there any sort of, I guess I
21 would call them information paths, that go missing
22 that you haven't mentioned already in response to
23 Board Member Liebert's observation about the ad tech
24 system?

25 DR. ZIMMECK: Yeah. I think one of the

1 points, if I'm correctly informed, it's the way that
2 in California, if, for example, someone is logged in
3 with their account, you know, then the opt-out
4 applies to also the mobile app, if they're logged in
5 on the website, for example; right? So I think if
6 that is known, then I think that would be good, you
7 know, to apply to, you know, these different, you
8 know, contexts. And I mean, if that's not the case,
9 then I do think -- and I mean, there was the earlier
10 effort on amending the CCPA with the mobile opt-out
11 setting; right? And so at the moment, what we have
12 is -- we have the -- you know, if you use an Android
13 or an Apple phone, for example, you have a way to
14 disable the advertising ID. And so that is basically
15 this idea that you -- as a developer of an app, you
16 agree with Google or Apple that you say, I -- when
17 somebody on their phone makes this ad ID setting, I
18 will not track them.

19 But that does not have the force under
20 the law. This is just a purely, you know,
21 contractual obligation that an app developer has
22 towards the companies. And so what we suggest is
23 that actually, this setting -- you know, this ad ID
24 setting should be actually relevant under the law.
25 You are actually declaring you opt-out under the law

1 when you make that setting. Because at the moment,
2 you have these two parallel tracks. You have the ad
3 ID opt-out, which has no meaning under the law. And
4 then you have the, you know, opting out under the
5 CCPA, for example, which is a separate interface
6 inside the app, which, by the way, half of all apps
7 do not have. And so, so I think my view, an urgent
8 problem is the opting out on mobile apps. I think
9 that is currently happening insufficiently. And
10 also, the situation is confusing for users because
11 you have these two up out systems that don't align
12 with each other.

13 CHAIR URBAN: Thank you. That's very
14 helpful. Thank you very much.

15 Are there additional questions from board
16 members? If not, well, thank you again, Dr. Zimmeck,
17 for that really enlightening presentation. It was
18 very helpful. I invite you to stay and listen. But
19 if you can't, we understand. And any public
20 comments, we will have recorded in transcripts and in
21 video in case that is of interest. So thank you
22 again very much. And we appreciate it.

23 DR. ZIMMECK: Yeah. Thank you. Also, I
24 want to say thank you to you. You know, it's such a
25 great thing that you do your work. And I'm always

1 happy to see the news, you know, coming out of
2 California. So thank you.

3 CHAIR URBAN: Well, we have a lot of
4 brilliant and extremely hard working people in the
5 CPPA who absolutely deserve that. Thanks. And I'm
6 sure they appreciate it. So thank you.

7 With that, we will move to our next
8 presenter, Mr. Daniel Goldberg. He is attorney and
9 chair of the data strategy, privacy and security
10 group at Frankfurt Kurnit Klein and Selz.

11 Mr. Goldberg advises companies on compliance with the
12 CCPA and other state privacy laws, with a focus on
13 advertising technology, online tracking, opt-out
14 rights, and data governance. He also represents
15 clients in privacy regulatory investigations and
16 enforcement matters. In 2025, the California Lawyers
17 Association named him California Privacy Lawyer of
18 the Year. Congratulations, it's a big honor.

19 Mr. Goldberg's presentation today will provide a
20 practitioner's perspective on opt-out preference
21 signals under the CCPA and explain the role of
22 pseudonymous profiles in the advertising technology
23 system and practical compliance considerations that
24 businesses face.

25 So, welcome Mr. Goldberg, and please do

1 begin when you're ready. Do you have slides?

2 MR. GOLDBERG: I do not have any slides.

3 CHAIR URBAN: Oh, that's --

4 MR. GOLDBERG: Just going to be speaking
5 to the Board.

6 CHAIR URBAN: Okay. That's absolutely
7 fine. I just wanted to be sure you had everything
8 you needed.

9 MR. GOLDBERG: I have everything here.
10 You can hear me fine?

11 CHAIR URBAN: Yes.

12 MR. GOLDBERG: Okay.

13 CHAIR URBAN: Go ahead.

14 MR. GOLDBERG: Excellent. Good afternoon
15 Chair Urban and members of the Board. Thank you for
16 inviting me here to participate today. I chair the
17 data strategy, privacy, and security group at
18 Frankfurt Kurnit Klein and Selz. I advise businesses
19 on CCPA compliance, including the implementation of
20 opt-out preference signals, and I do a significant
21 amount of work in advertising technology.

22 I am here to offer a practitioner's
23 perspective on opt-out preference signals,
24 specifically the role of pseudonymous profiles in the
25 advertising ecosystem and the practical compliance

1 considerations that businesses face when honoring
2 these signals. And I'm speaking today in my
3 individual capacity, based on my own experience
4 advising clients as a lawyer, and not on behalf of
5 the firm or on behalf of any specific client. I have
6 to put that out there.

7 So let me start by looking at the CCPA
8 rule itself that we're talking about. When a
9 business receives an opt-out preference signal, the
10 regulation requires the business to treat that signal
11 as an opt-out at three levels. The first level, the
12 business, must apply the opt-out to the specific
13 browser or device. The second level, the business
14 must apply the opt-out to any consumer profile
15 associated with that browser or device, including a
16 pseudonymous profile. And third, the business must
17 apply the opt-out where the consumer is known to the
18 business.

19 So for this last example, the
20 known-to-the-business, the attorney general's
21 settlement earlier this year illustrates this known
22 consumer case. And Stacy's going to be talking --
23 I'm sure -- about this a little bit later. In that
24 case, the attorney general alleged that Disney
25 offered a single account through which consumers

1 could access Disney+, Hulu, and ESPN+ on televisions,
2 phones, tablets, and computers. According to the
3 complaint, Disney used data associated with those
4 accounts for advertising across its services, but it
5 did not fully apply consumer opt-outs across the
6 devices and services connected to those accounts.

7 The complaint explained how the attorney
8 general applied the regulation to those facts. And
9 to quote the complaint, "If a business can associate
10 a consumer's devices with the consumer for
11 advertising purposes, it can and it must use those
12 devices with the consumer for purposes of honoring
13 the consumer's opt-out rights." Put another way, if
14 a business relies on an association to obtain the
15 benefits of advertising across devices, it must also
16 account for that association when applying the
17 consumer's opt-out. So Disney is a relatively
18 straightforward application of that rule. Through
19 the consumer's account, Disney already had a way to
20 connect consumer activity across devices and
21 services. But the harder question arises when there
22 is no known consumer and no account connecting that
23 activity. In that situation, the regulation still
24 requires the business to apply the signal to any
25 associated consumer profile, including a pseudonymous

1 profile, which I'm now going to talk about.

2 And to understand why the Disney
3 principle becomes harder to apply in that setting, it
4 helps to understand and look at how advertising
5 systems work. At a high level, the advertising
6 ecosystem connects publishers that have ad space with
7 advertisers that want to reach relevant audiences.
8 Various ad tech companies may select the
9 advertisement, deliver it, provide audience
10 information, or measure the results.

11 Much of online advertising does not
12 depend on knowing a consumer's name. Instead,
13 advertising systems recognize a browser or device
14 through what the CCPA calls a unique identifier,
15 which includes identifiers such as cookie IDs, mobile
16 ad IDs, IP addresses, and other device identifiers.
17 For example, an advertising company may assign a
18 browser an identifier such as ABC123. That
19 identifier allows the company to recognize the
20 browser, but not on its own identify the specific
21 consumer using it. It therefore functions as what I
22 would call a pseudonymous identifier. Over time, the
23 company may record activity under that identifier.
24 For example, when a browser visits a web page,
25 receives an advertisement, or completes a purchase,

1 the company may store that event in its systems using
2 the identifier. This allows the company to collect
3 information such as browsing activity, inferred
4 interest, ads shown, audience segments, or purchase
5 activity, to the same identifier.

6 Now, advertising systems may connect
7 identifiers and activity in more than one way. Some
8 connections are direct, where one identifier is
9 directly mapped to another identifier. Other
10 connections are inferred from patterns or signals
11 with varying degrees of confidence. And each company
12 often uses its own proprietary identifier. So a
13 publisher's web page may include advertising
14 technologies from several companies, each of which
15 places its own cookie and assigns its own browser and
16 identifier, which is proprietary. So cookie syncing
17 is a method, it's a direct method, of linking these
18 different identifiers, and is a useful one for us to
19 walk through right now.

20 In cookie syncing, two companies assign a
21 unique identifier to the same browser. For example,
22 company A may assign the browser the identifier
23 ABC123, while company B independently assigns that
24 same browser XYZ987. Because each company cannot
25 directly read the identifiers stored in the other

1 company's cookie, neither initially knows that the
2 two identifiers relate to the same browser. When the
3 browser loads a page involving both companies'
4 technologies, one company may direct the browser to
5 send a request to the other that includes the
6 identifier, so the receiving company can then match
7 the identifier to its own and store the relationship.
8 So ABC123 maps to XYZ987 for that browser. That
9 mapping allows companies to recognize that their
10 different identifiers refer to the same browser and
11 use the information connected to those identifiers
12 for advertising activities. So this brings us right
13 to the practical compliance considerations businesses
14 face when getting opt-out preference signals and
15 looking at the regs.

16 So when you look at the regs, the regs
17 talk about pseudonymous profiles, but they don't
18 define it and they don't explain what it means for a
19 profile to be associated with a device or a browser.
20 When counseling clients, I think of a pseudonymous
21 profile as a pseudonymous identifier together with
22 the information collected with it. So the identifier
23 functions as the key through which the business
24 recognizes and retrieves the information under the
25 profile. The harder question is, what makes that

1 profile associated with the browser or device that
2 sends the signal?

3 In the cookie sync example, the
4 connection is direct. One identifier is directly
5 mapped to another identifier used for that same
6 browser. However, not every association is based on
7 a direct identifier match. The CCPA recognizes the
8 concept of an inferred association through its
9 definition of a probabilistic identifier, which is an
10 identifier that identifies a consumer or device to a
11 degree of certainty that is more probable than not.
12 That definition does not necessarily determine what
13 "associated with" means, but it does suggest that an
14 inferred association requires more than a possible or
15 speculative connection. For businesses, the
16 practical difficulty is determining when an inferred
17 connection is sufficiently reliable to be treated as
18 an association for purposes of applying the signal.

19 Now, this reliability of an association
20 can change over time, including an association
21 originally established through a direct match.
22 Cookies expire or may be deleted. IP addresses can
23 change or be reassigned. Mobile ad IDs may be reset
24 or become unavailable, and patterns of activity may
25 become stale. As those underlying identifiers and

1 signals change, an association that was once reliable
2 may no longer reflect the same consumer or device.
3 In that context, businesses therefore have to
4 translate the regulation's language into practical
5 questions. What profile does the business actually
6 maintain? What connects that profile to the browser
7 or device sending the signal? How reliable and
8 current is the association? And does the business
9 actually use or rely on that association for
10 advertising purposes?

11 Now once a business has identified the
12 relevant profile and association, it still faces the
13 difficult task of actually operationalizing the
14 opt-out across its systems. The first challenge is
15 detecting the signal and translating it into an
16 actionable preference within the business's systems.
17 Most businesses rely on a consent management
18 platform, or CMP, or another outside vendor to
19 perform that function. Now, these products can be
20 expensive and their capabilities vary considerably.
21 Many consent management platforms were originally
22 designed to address the opt-out at the browser or
23 device level only, for example, by detecting the
24 signal on a particular website and preventing
25 selected advertising technologies from operating

1 there. But that does not necessarily mean that the
2 platform can apply the opt-out to every consumer
3 profile associated with that browser or device, or to
4 a known consumer. And although these products are
5 often marketed as tools for CCPA compliance, broader
6 functionality may require a higher-priced tier, an
7 additional module, custom configuration, separate
8 engineering work, or another vendor altogether. Even
9 then, the platform may only pass the preference to
10 systems that have specifically been integrated with
11 it. And even when the preference is successfully
12 captured, the business still has to route it to the
13 relevant profile and data uses that exist.

14 That can be difficult because businesses
15 often operate through fragmented technology
16 environments. They may use different advertising
17 platforms, separate accounts and audience systems,
18 legacy databases, systems inherited through
19 acquisitions, or different technologies across brands
20 and business units. Some of those systems may
21 communicate through a shared database or vendor, and
22 others may use different identifiers or not
23 communicate at all. So, as you can see, there's a
24 lot going on here, and that requires the business to
25 ask practical questions about its systems and work

1 through the operations. Does one system recognize
2 the identifier used by another? Is there an account,
3 shared database, common vendor, or other existing
4 relationship that connects them? Or would the
5 business actually have to go and create a new
6 identity resolution process solely to establish this
7 connection? Those questions point to an important
8 distinction between honoring an association the
9 business already maintains and requiring the business
10 to create an association that does not otherwise
11 exist in its systems.

12 So consistent with both the regs and the
13 Disney case, the obligation should really extend to
14 connections that the business actually uses and
15 relies on. So if it uses a connection for
16 advertising, it must account for that same connection
17 when applying the opt-out. But if it does not
18 maintain or rely on that connection, it should not
19 have to create a new identity resolution process
20 solely to expand the signal's reach.

21 So, one way the Board can provide
22 practical guidance on honoring opt-out preference
23 signals for pseudonymous profiles would be through an
24 example, such as a cookie sync example. Returning to
25 our earlier example, let's assume business W uses the

1 unique identifier ABC123 for a browser, and business
2 X uses the identifier XYZ987 for that same browser.
3 Business W's website facilitates a cookie sync in
4 which ABC123 is transmitted to business X. Business X
5 then directly maps ABC123 to XYZ987. That mapping
6 creates a direct association between the browser
7 identified by ABC123 and the pseudonymous profile
8 consisting of XYZ987 and the information connected to
9 it. A consumer visits W's website, now using a
10 browser that has an opt-out preference signal
11 enabled. If business W receives the signal before
12 the cookie sync occurs and can prevent the
13 transmission, it should not initiate the sync with
14 business X. If the cookie sync has already occurred,
15 business W would need to stop further transmission of
16 ABC123 to business X or communicate the preference to
17 business X.

18 An example could also address how the
19 reliability of an association may change over time.
20 As I mentioned, a cookie may expire or be deleted, an
21 IP address may be reassigned, a device may change
22 hands, or a probabilistic link may become stale. The
23 historical association may remain stored, but it may
24 no longer reliably connect the browser or device to
25 the same pseudonymous profile. Additional guidance

1 would be helpful on how the opt-out applies when the
2 association is no longer sufficiently reliable or
3 current. This would give businesses practical
4 guidance without requiring the regs to adopt a
5 comprehensive definition of pseudonymous profile or
6 "associated with."

7 So in closing, my hope was to give the
8 Board a practical overview of how businesses think
9 about operationalizing opt-out preference signals and
10 the complexities with it. And I really do think that
11 Disney provides a useful guiding principle. If a
12 business relies on an association for advertising, it
13 must also account for that association when applying
14 the opt-out. At the same time, as this discussion of
15 pseudonymous profiles shows, translating that
16 principle into practice is difficult. A concrete
17 cookie example could help illustrate how the rule
18 applies when a browser is directly associated with a
19 pseudonymous profile. And additional guidance would
20 also be helpful on how the opt-out applies where an
21 association is no longer sufficiently reliable or
22 current, and on the distinction between honoring an
23 existing connection and requiring the business to
24 create a new identity resolution process.

25 So, thank you very much. I know I've

1 said a lot, and I'm happy and welcome to answer any
2 questions the Board may have.

3 CHAIR URBAN: Thank you very much,
4 Mr. Goldberg.

5 Questions from the Board?

6 Go ahead please, Board Member Liebert.

7 MR. LIEBERT: Wonderful presentation,
8 Daniel. I want to go a little bit higher than the
9 weeds that you've been in about pseudonymous -- if I
10 can pronounce it -- profiles in about 30,000 feet, as
11 you're one of the State's honored privacy lawyers.
12 Have you become a luddite now that you know so much
13 about what's happening in -- with our personal
14 information in these ads? You don't have to answer
15 that.

16 Okay. Here's my question. The ad tech
17 world has obviously been brilliant in finding ways to
18 discover who we are for purposes so -- of selling
19 things to us. I'm wondering what you tell your
20 friends and family as to whether it's actually
21 possible now given that there are dossiers on all of
22 us as to who we are. I mean, years have gone by,
23 right, where all of this information has been scooped
24 up. Is it too late, or do you feel like there are
25 things that we can still do and that we're all trying

1 here in this Agency so strongly to really start
2 shutting off that spigot in a way that will protect
3 California's consumers?

4 MR. GOLDBERG: So one interesting things
5 about the advertising ecosystem and especially on the
6 legal side -- I'll speak on that -- is I find that
7 especially the lawyers who think about this in the
8 advertising ecosystem are really sophisticated and
9 dig into these issues. And I'm part of several trade
10 organizations, and they're really wonderful about
11 thinking about these issues. I do not think it is
12 too late to be thinking about this at all. I also
13 think tremendous strides have been taken with respect
14 to things. I mean, a good example is what's going on
15 with the Delete Act, right, and data broker
16 obligations as well, which has an impact on all this
17 stuff that's going on. So no. And that's why I'm
18 saying that I think thoughtful interpretation of what
19 the regs requires is really important where it's not
20 like a one size fits all rule. It's really looking
21 into the specific facts of what's going on.

22 CHAIR URBAN: Thank you.

23 Board Member Hamer, please?

24 MS. HAMER: Yeah. So I think I was
25 following everything you said without slides.

1 MR. GOLDBERG: I know it's a lot. Yeah.

2 MS. HAMER: Yeah. No. I'm just curious
3 how what you're describing is different or more
4 complicated than the data governance and data
5 cleansing and data management issues that all
6 businesses who are subject to CCPA have to go
7 through, for example, when they get a deletion
8 request. Because you've got last name first, first
9 name last, some dots. So you've got the same kind of
10 issue, and everybody seems to be able to do it. So
11 help me understand.

12 MR. GOLDBERG: So -- and this kind of
13 goes back to the known consumer point that I was
14 saying. That if you have an account on a known
15 consumer and you receive a deletion request, right --
16 so it's Jill Hamer, first name, last name, or email
17 address, it's not that difficult to go into your
18 system potentially and purge that. And I think
19 that's really like the intent of everything we're
20 looking at. When you're looking at these identifiers
21 and these pseudonymous profiles, they're not always
22 directly connected to that level. And as I was
23 mentioning, they have different levels of, you know,
24 how connected they are with the levels of
25 association. And so it becomes a very technical

1 process. And in my experience, the companies I've
2 worked with really do try to comply with this. They
3 work very diligently to delete data or to opt-out
4 from their systems. But not all systems talk to each
5 other. You're working with a lot of different
6 vendors, for example, and you may have two different
7 identifiers that are completely unrelated. And so
8 that's kind of the question is, how do you think
9 about that, operationalizing it when it's not a known
10 consumer? And that -- right? Like, when it's not
11 directly connected to this individual. And the law
12 says there are still responsibilities around that
13 data set.

14 CHAIR URBAN: I'd like to follow this up
15 by pressing you a little bit. I'm quite sympathetic
16 to the messiness of the situation for businesses, and
17 I certainly hear what you're saying about the
18 probabilistic connection and that there is a point
19 where the probabilities become pretty loose. I
20 understand the practicality, and it makes sense to me
21 that it -- and I will say at a minimum, if the
22 business understands or relies on that, that is an
23 identifier that counts. What I need help with is
24 what is your line for when it doesn't count. And if
25 you have an example, that would be great. And it's

1 similar to Board Member Hamer's question.

2 Businesses, you know -- well, so that's one question.

3 And then relatedly, I'd like to
4 understand why this is more difficult for businesses
5 than the current situation where, for example, if I
6 trash all my cookies and I trash all my trackers, I
7 know I have to start over. As a consumer, I know
8 that the browser is going to go to the site. The
9 site's not going to know who I am anymore, and I'm
10 going to have to start over. And so that seems to be
11 built into the ecosystem, that kind of understanding,
12 at least at that level. I recognize once you have
13 these many, many transactions between many, many
14 parties, it gets exponentially or at least maybe
15 something between monotonically and geometrically.
16 -- sorry to be a nerd -- more complicated very
17 quickly.

18 But I'm -- what I'm trying to understand
19 is, where do you think is the reasonable line of
20 connection probabilistically? Because I'm just not
21 quite with "if the business understands and relies
22 on," because that changes dynamically over time. And
23 I think what I would like to look for is something
24 that is implementable by businesses and also meshes
25 with consumer expectations. And to the extent that

1 requires businesses to keep track of how their
2 systems are operating and to change the way they are
3 treating these pseudonymous identifiers when they've
4 updated the system in some way so that the
5 probability changes. I would like them to do that,
6 because that messes more closely with consumer
7 expectations. And that is more privacy protective,
8 which is what the law is really asking businesses to
9 do.

10 So if you can give me a sense of what you
11 think is reasonable, like what's too loose a
12 connection, probablistically, what's reasonable.
13 And, you know, where is the line, I guess, on what
14 businesses responsibility should be?

15 MR. GOLDBERG: So those are great
16 questions. And it's what makes it difficult to
17 answer that easily is that ad tech is really complex.
18 And every company, I know that it's generalization,
19 but --

20 CHAIR URBAN: No, no. I'm sorry. I
21 didn't mean to talk over you. It is. It is
22 exceptionally complex.

23 MR. GOLDBERG: It is exceptionally
24 complex. And so every company has its different
25 methods of how it connects identifiers, how it

1 crosses it. And as I mentioned when I was speaking
2 before about probabilistic identifier, again, that is
3 actually in the CCPA underlying text.

4 CHAIR URBAN: Right. I know. And even
5 though that it's not defined, we don't know how --

6 MR. GOLDBERG: Well, probabilistic --
7 sorry.

8 CHAIR URBAN: -- needs to be -- right.
9 What I'm asking is, if the regulations don't give
10 sufficient guidance on how close the connection
11 becomes, what guidance should we give?

12 MR. GOLDBERG: I think it's, it's one
13 that probably examples would help. I think it's
14 really hard to give a specific clear line of here is
15 what the answer is or not. That's just, you know,
16 the reality of the situation. And there has to be
17 some level of room there that, you know, our goal --
18 and I agree with you completely -- is to facilitate
19 the protection of consumers, but also in a way that
20 actually, you know, businesses can comply with. And
21 so what I think -- you don't want to have something
22 that is so stringent that no one can comply with it.

23 CHAIR URBAN: So can you give me an
24 example of when a business can not comply? Maybe
25 let's start there.

1 MR. GOLDBERG: Yeah. So a good example
2 would be that you have, you know, maybe a system in
3 place where you have two systems that, like, don't
4 talk to each other at all, and they're both wings of
5 the business that engage in advertising practices.
6 So what I'm saying is that if those are not connected
7 and the business is not getting the benefit of that
8 data to reidentify. And to connect those two systems
9 completely is a really difficult task. And I
10 actually think, you know, within the confines of the
11 law, the way I read it, it would require a lot on
12 behalf of the business.

13 CHAIR URBAN: So sorry, just to pause to
14 make sure I understand. So let's say we have two
15 divisions or we actually have two -- we have two
16 subsidiaries and --

17 MR. GOLDBERG: Yeah.

18 CHAIR URBAN: -- do different things.
19 And a consumer opts out or sends a preference signal
20 to one subsidiary. And the other subsidiary over
21 here also has some kind of pseudonymous identifier
22 that would go with that person's device or maybe with
23 the person themselves, and then asking them to find
24 that match --

25 MR. GOLDBERG: To find that match.

1 Exactly.

2 CHAIR URBAN: -- would be difficult. So
3 how does this connect to Board Member Hamer's
4 question about data governance, generally. Should we
5 not expect businesses to have this kind of
6 communication, because this is a known person.

7 MR. GOLDBERG: No, of course. And so
8 data governance, right, is the concept of saying that
9 you have to have -- like, you have to be thinking at
10 a high level, what you're looking at and how you're
11 addressing privacy compliance. But I think that
12 requiring that affirmative connection when there is
13 not a connection, can be something that is almost
14 impossible for a business to do it, unless they had
15 like a similar vendor that was connecting, you know,
16 the two processes there --

17 CHAIR URBAN: Okay.

18 MR. GOLDBERG: -- between the
19 identifiers.

20 CHAIR URBAN: I thought you were going to
21 go to relationships outside of one business entity to
22 another entity. So now I'm sorry. This is not --
23 you have my academic antenna up.

24 MR. GOLDBERG: No, no. Of course.

25 CHAIR URBAN: So how then would you

1 evaluate the same subsidiary but with multiple
2 divisions that have sort of different
3 responsibilities and they attract some set of -- two
4 sets of customers with an overlap, but they're not
5 all the same customers. Should they be able to --
6 should they -- do they have enough information and
7 reliance in order for that to be --

8 MR. GOLDBERG: Yeah.

9 CHAIR URBAN: -- actionable?

10 MR. GOLDBERG: Absolute. So if it's
11 relating to the known consumer; right? So I think,
12 again, going back to the Disney example, there's a
13 login. If it is connected in that way between these
14 parts of the organization, that you can associate
15 everything, I do think so. But I think if you have
16 two separate systems and you get -- you know, you get
17 the signal, let's say, the GPC signal coming in, and
18 it's relating to a specific identifier. And that
19 identifier is connected to one data set, but not the
20 other, there's no way for the business necessarily to
21 associate that with the other side of it. That's
22 what I'm saying.

23 CHAIR URBAN: And then when you add the
24 probabilistic profiling in the middle, so that
25 there's some information, you know, you can't do the

1 one-to-one if you -- I think it was ABC 123. And
2 BB --

3 MR. GOLDBERG: Yeah, yeah, yeah.

4 CHAIR URBAN: It's not one-to-one, but
5 there's a probabilistic cloud of some sort. How
6 should we treat that, going beyond if the business
7 relies on it and has understanding. What's the --
8 how -- what is the probability or the reliability
9 that you would think was reasonable?

10 MR. GOLDBERG: So in -- when I go back to
11 the definition, it says more probable than not. So
12 that's how I would be looking at it.

13 CHAIR URBAN: Okay. All right. So that
14 itself is not too challenging in the regulations, but
15 examples would be helpful.

16 MR. GOLDBERG: Exactly.

17 CHAIR URBAN: Okay. Thank you very much.

18 MS. HAMER: Okay.

19 CHAIR URBAN: Yes.

20 MS. HAMER: I'm still a little confused.
21 Because you were talking about a business having two
22 different systems that don't talk to each other,
23 which seems a little archaic to me given the other
24 privacy rights that are going on. Like, what would
25 you --

1 MR. GOLDBERG: You'd be shocked.

2 MS. HAMER: No, I actually wouldn't. But
3 I -- you know, I shouldn't be. We've been around for
4 a while. And businesses have had plenty of notice to
5 get their data management and data government stuff
6 together. So what would you advise the one company
7 that has two different systems that don't talk to
8 each other, but share some client data?

9 MR. GOLDBERG: I think that's the key --

10 MS. HAMER: Not ad data, but, you know,
11 data deletion. The data deletion is a basic request.

12 MR. GOLDBERG: I think -- by the way, I
13 want to be very clear. That's the key. It's the
14 fact that you're talking about the sharing of the
15 data that connects it -- that allows for the
16 connecting of it, the association. In that case,
17 you're getting the benefit of the data for the
18 advertising purposes. That's what I'm saying is that
19 if it's -- you know, you're looking at like the
20 chain. If the chain is connected, it's much easier
21 to be able to facilitate that than if it's completely
22 separate.

23 MS. HAMER: I'm still not sure --

24 MR. GOLDBERG: Yeah.

25 MS. HAMER: -- that we're talking about

1 the same thing.

2 MR. GOLDBERG: Okay.

3 CHAIR URBAN: I think process-wise, I'm
4 not sure a Board Member Hamer is talking about
5 exactly the same thing as Mr. Goldberg. I also --
6 Mr. Goldberg, tell me if this is wrong. I got a
7 sense that you have practical pushback to the idea
8 that within the same company, the systems really are
9 -- can reasonably, easily be connected to each other.

10 MR. GOLDBERG: That is correct.

11 CHAIR URBAN: Yes. And with opt-out
12 preference signals, you often have pseudonymous --

13 MR. GOLDBERG: Yes.

14 CHAIR URBAN: Good heavens -- and so
15 forth, which is a little bit different from other
16 kinds of relationships with the business. This is
17 how I understand the essential problem space.

18 MR. GOLDBERG: Yes.

19 CHAIR URBAN: Okay. Thank you. So I
20 think -- to Board Member Hamer and to all of us, one
21 thing we could think about certainly would be to come
22 up with examples, as Mr. Goldberg suggests. And then
23 we would receive public comment that I hope would be
24 very concrete about how practical they are. And we
25 would hear from businesses, of course, but also

1 consumers in civil society groups about where they
2 think the opt-out breaks, when it should not. I'm
3 not asking anybody to agree with me in the
4 information session. I'm just trying to repeat back
5 to you what I understood you to say the problem to be
6 and some of the ways that we might address it.

7 Any other comments or questions from the
8 Board?

9 Board Member Ozer?

10 MS. OZER: Thank you so much. Yeah. I'm
11 just trying to kind of zoom out a little bit as well,
12 and just sort of -- whose burden it is when there is
13 more complexity? Because I'm also sort of hearing
14 this a little bit, that, you know, consumers have
15 some rights or some opportunities or some tools to
16 better protect their privacy. But then, of course,
17 the companies want to continue to do advertising. So
18 then the system becomes more complex in terms of sort
19 of finding ways that that profit can still happen,
20 even though there are some regulations or laws in
21 place. And so I'm just -- there's sort of specific
22 compliance, and then there's obviously like privacy
23 guidance and sort of bigger picture governance.

24 So I am hearing you that there's a lot of
25 complexity and, you know, as a lawyer myself, I

1 understand that, you know, then you're kind of
2 helping your clients figure out how to then navigate.
3 But I guess the question for me is how much of this
4 complexity is being created on the company's side in
5 order to continue to do things that maybe the intent
6 is to try to address.

7 MR. GOLDBERG: So first off, to be clear,
8 I mean, I do think the burden should be on industry
9 and on companies. Like, I'm in no way disputing
10 that. And that's my own personal belief. A lot of
11 the systems were created with the concept in mind
12 that the advertising industry did not necessarily
13 want to recognize the individual consumer. It was
14 more focused on getting the right ad to the right
15 device. And a lot of it is using like legacy
16 systems, as I was mentioning, where you'll have the
17 company acquires another company, and the two systems
18 don't talk to each other, et cetera. And so that's
19 part of it, is that all, you know, what I'm saying,
20 -- and I agree -- is that the business really needs
21 to look at this, and in no way can they disregard
22 what the obligations are. At the same point, it's --
23 you know, it's the -- how specific it is and what the
24 regulations are laying out. And these are the
25 different elements that businesses are thinking about

1 all the time and how they address it.

2 MS. OZER: I guess one of the questions
3 is just sort of a specific compliance versus a system
4 approach. Our goal here is actually to respect sort
5 of the privacy -- the expectations of the consumer
6 versus, okay, we have these really technical systems
7 and, you know, parsing of the language in terms of
8 specific compliance. So I'm just interested in sort
9 of when you see something like this kind of legacy
10 system, what is the kind of practical advice you
11 give? Are you giving more like, well, let's look at
12 this systematically.

13 MR. GOLDBERG: Well, we -- I mean, I
14 always look at it, to the extent you, you know,
15 really, you can be doing it, you should be doing it.
16 Like, that's a big part of this is recognizing that
17 people have the right to their privacy and to be
18 protected. And I think when you look at the law
19 around the association language that says, you know,
20 associated with the pseudonymous profile, device
21 associated, that's what it hangs on, is what is that
22 association? And to Chair Urban's point, you know,
23 that's the question is, what triggers that? What
24 level of association is that? And that's a really
25 difficult thing for businesses to look at that.

1 CHAIR URBAN: It's possibly less
2 difficult for businesses if they are taking a systems
3 approach that is privacy first. Because then the
4 association will -- they, they won't need to split
5 hairs over how close the association is if they are
6 first considering whether or not that's the -- if
7 they're -- excuse me -- if they're using privacy as a
8 default.

9 MR. GOLDBERG: Of course. And again, if
10 the associations are being used in a way for
11 advertising purposes where they're connected in that
12 way, I -- again, I completely agree.

13 CHAIR URBAN: Yeah. And I absolutely
14 take the point about the technical difficulty with a
15 specific compliance as Board Member Ozer put it. And
16 I'm sure businesses want to feel comfortable that
17 they are doing what they need to do, in case there's
18 an enforcement attention from the Agency. And so
19 certainly, these questions aren't simple, however you
20 look at it. But I do agree with Board Member Ozer
21 that the defaults do help as well.

22 But I really -- Board Member Liebert, did
23 you have another question? And then I think we
24 really -- we're going to need to let Mr. Goldberg go,
25 who's been very patient with us.

1 MR. LIEBERT: Let's keep him patient. In
2 your practice, what percentage of folks are doing
3 these pseudonymous profiles? Because I think so many
4 consumers are so confused about how to -- even how
5 the systems work, how to protect their information.
6 We're making some strides with the Delete Act now.
7 But I -- is this something that's actually very
8 prevalent that the companies are dealing with?

9 MR. GOLDBERG: So as you are probably are
10 aware, companies have -- oftentimes if you're a
11 publisher, advertiser, you have many tracking
12 technologies on your website. And so that's why I
13 think, you know, the cookie sync is a good example,
14 that you may have two companies that have a
15 technology, and they each drop their own identifier.
16 They don't really talk to each other. And then the
17 cookie sync allows you to match that. So the answer
18 is it's really dependent on the website and the
19 company. There's a lot of this in the ecosystem. A
20 lot of it is honestly even much more basic, that it's
21 just like we have trackers, and it looks at that
22 specific device. So it's really dependent on, on
23 kind of the company.

24 CHAIR URBAN: Thank you, Mr. Goldberg.
25 It really was an absolutely stellar walkthrough of

1 the way the communications happen between the
2 different systems that you did for us. I found it
3 really helpful and enlightening, and I see where the
4 seams are. I think that it has been extremely
5 helpful to hear where the seams are from the
6 perspective of your clients. And hopefully, that
7 will help us provide guidance that will be useful in
8 some form. So thank you very much.

9 MR. GOLDBERG: Thank you to the Board for
10 your time today.

11 CHAIR URBAN: Does anybody need a quick
12 break, or shall we? Yes, no. Okay. All right. We
13 have our next presenter, I believe, is also remote.
14 Is our technical system for that in place, or should
15 we take a small break for technical checks. Okay.
16 Wonderful. Thank you again to Mr. Goldberg.

17 Our next presenter is Dr. Christo Wilson,
18 professor in the Khoury College of Computer Sciences
19 at Northeastern University. Dr. Wilson is a founding
20 member of the Cybersecurity and Privacy Institute at
21 Northeastern, and he serves as the associate dean for
22 undergraduate programs at Khoury College. His
23 research covers a wide range of digital consumer
24 protection topics using measurement-driven
25 approaches. This includes areas like online tracking

1 and privacy, deceptive dark-pattern user interfaces,
2 misinformation and radicalization, fairness and bias
3 in machine learning, algorithm auditing, and
4 empirical antitrust investigations of tech platforms.
5 Dr. Wilson is co-PI of the National Internet
6 Observatory, which is a National Science Foundation
7 funded project gathering data about the online habits
8 of a large representative panel of US residents. The
9 observatory makes this data available to qualified
10 researchers around the world. He will be speaking on
11 the where and when of consent and GPC for
12 Californians, Global Privacy Control. This session
13 will highlight two technical issues regarding the
14 timing and ambiguity of consent signals and how
15 Global Privacy Control helps publishers address these
16 challenges.

17 Welcome, Dr. Wilson. Thank you for
18 joining us and for offering us your expertise, and I
19 will turn things over to you.

20 DR. WILSON: Well, thank you very much.
21 It is my pleasure and honor to be here. I do have
22 some slides to share.

23 CHAIR URBAN: Sure.

24 DR. WILSON: Is that showing the correct
25 screen? Is that thing presenter mode? I'm also

1 getting a lot of echo.

2 CHAIR URBAN: They are in the control
3 booths. They are working on getting your slides into
4 presenter mode. Bear with us.

5 DR. WILSON: I think I can fix this on my
6 end. One moment.

7 CHAIR URBAN: There we go. That looks
8 good.

9 DR. WILSON: There we go. All right.
10 Thank you very much.

11 CHAIR URBAN: Yeah. It looks great from
12 here. If it looks good on your end, please go ahead,
13 Dr. Wilson.

14 DR. WILSON: I apologize for the hiccup,
15 and thank you again for having me. It's a pleasure
16 to be here. So I've already been introduced. I'm
17 Christo. I'm a computer scientist by training, and
18 my research focuses on digital consumer protection
19 issues.

20 Around 2021 is when I first got
21 interested in the CCPA, because it was an incredibly
22 important landmark privacy law in the United States.
23 So at the time, we were really interested in how
24 websites were complying with the law, and our focus
25 was on the "do not sell my personal information"

1 links that websites were supposed to include. So,
2 here's an example of one from West Elm; right? The
3 idea is that websites were supposed to have this
4 link, people could click it, and in doing so activate
5 their privacy rights under the law. So we conducted
6 a large-scale study where we ran web crawlers, we
7 tried to find these links on websites, and this led
8 to some interesting findings looking at whether those
9 links were clear and conspicuous as the law requires.
10 One of the things we looked at is whether the sort of
11 size and font of those links was good enough, and it
12 turns out that around 50% of all those links were
13 either too small or too faint to be reasonably
14 accessible.

15 Another thing we looked at is where the
16 links appeared on web pages. On the right, this
17 black rectangle is a heat map showing where links
18 were on web pages, and most of it's black, but
19 there's this very hot area at the bottom. You know,
20 unsurprisingly, it turns out that most of the
21 websites that had adopted this link put them at the
22 very, very bottom, in the footer of the page. So our
23 takeaway from this study was that these links, when
24 they were being adopted, were not really clear and
25 conspicuous enough. And so that brings me to the

1 topic of Global Privacy Control. I'm grateful to
2 Professor Zimmeck for really introducing the concepts
3 here.

4 So one thing I'd like to start off by
5 saying is that GPC solves a lot of these usability
6 challenges that we saw with those links. When a user
7 adopts GPC and enables it in their browser, there's
8 no longer a need for them to hunt around on a website
9 for this little obscure link. There's potentially no
10 need for them to be interrupted by a big complex
11 banner. And by eliminating these sort of roadblocks,
12 right, this reduces the opportunity for dark
13 patterns. So this is something we've seen a lot in
14 research when we look at these kind of consent banner
15 interfaces. Here's an example in the screenshot
16 where there's a big "Accept All" button that's very
17 prominent, but to actually opt-out, there's no button
18 for that. You have to go to "Manage Cookies" and go
19 through a complex, adversarial process; right? So
20 GPC is wonderful in that it helps alleviate a lot of
21 those kind of user interface issues.

22 But what I want to spend most of my time
23 talking about is other ways that GPC helps,
24 specifically related to timing and ambiguity problems
25 that websites face. So I'm going to be using one of

1 my favorite websites, Penny Arcade, as an example.
2 It's a web comic. And if you pay attention to this
3 screenshot, you'll see a couple of important things.
4 So Penny Arcade is ad-supported; right? There's a
5 big advertisement on the right-hand side of the page.
6 But at the bottom, as a good citizen trying to comply
7 with the law, they have a cookie banner. This one
8 doesn't have any dark patterns there's a button for
9 "allow," and there's a button for "use necessary
10 cookies only," which is presumably the way the user
11 is supposed to opt-out. So in theory, the user, if
12 they want to opt-out, is supposed to click that
13 button, and then the publisher, in this case Penny
14 Arcade, is supposed to react. They're supposed to
15 stop selling and sharing data to third parties to
16 comply with the law.

17 There's a couple of different ways they
18 can implement that. Option one is to simply not do
19 it at all, maybe remove advertising and tracking from
20 the website entirely. Another option is to continue
21 using third parties, but don't sell or share data to
22 them. This is more of a data minimization approach.
23 Or option three is that the website can continue
24 contacting third parties, it can even send sensitive
25 data to them, but it can put them into a restrictive

1 service provider mode. This is sort of a data-use
2 restriction approach. All of these are fine and
3 would comply with the user's desire to opt-out.

4 So this all seems good in theory. User
5 clicks button, data is treated differently, but the
6 technical details really matter. And as it turns
7 out, there's a lot of ways that this can go wrong and
8 the user's choice can not be honored. So this brings
9 us to some of these issues with opt-out compliance.
10 I'll go through an example of web page construction
11 in a minute, but it's important to understand that a
12 website is not a monolith. It's actually composed of
13 hundreds of different objects that load one by one in
14 order, and it's the sum total of those objects that
15 compose a website.

16 We've already been introduced to the
17 concept of consent management platform, or consent
18 management software. This is often one of these
19 components that gets downloaded and inserted into web
20 pages while they're loaded. And the idea behind the
21 consent management software is that it's supposed to
22 implement a lot of this CCPA compliance
23 functionality, so it's often what presents these
24 banners to the user. If the user interacts with the
25 banner, that consent manager is supposed to collect

1 and store a consent signal, i.e. the user's choice to
2 opt-out, and then it's also then responsible for
3 acting on that consent signal, so stopping the
4 selling and sharing of data or restricting data
5 flows.

6 There's two particular problems with this
7 kind of overall approach that I want to highlight.
8 So one is, when is the consent signal available, the
9 timing component? The second is, where is the
10 consent signal located? This question of ambiguity.

11 So let's take it from the top. Websites
12 are not monoliths, they're composed of many small
13 objects, and they load incrementally. So while it
14 may appear that the website is available in the blink
15 of an eye, in reality there's a process going on. So
16 what typically starts with -- if you go and visit a
17 website, the first thing you'll get is the HTML.
18 That gives you kind of the overall structure of the
19 page and a lot of the content, like the text, but not
20 much else. Then you might start loading different
21 images, right, maybe then some other resources start
22 to load, like fonts, or third-party analytics, things
23 to track what you do on the site, look for bugs, that
24 kind of stuff. Then advertisements might load.

25 So now your browser is contacting

1 real-time bidding services, different ad networks,
2 ultimately contacting an advertiser, showing an ad.
3 And then eventually maybe the consent management
4 platform loads, and you get this cookie banner. So
5 eventually you have the whole website, but the timing
6 really matters here. And as you might have guessed,
7 I've constructed this example in a way to highlight a
8 particular issue. The third-party analytics and the
9 advertisement got loaded before the consent manager.
10 That is a problem that is all too common in reality.

11 So let's look at this in terms of a
12 timeline. On the bottom here, we have time going
13 from left to right. Your browser starts by
14 downloading the HTML of the web page. At some point
15 down the road, the consent management software loads.
16 From that point on, the user is able to click a
17 button and make a choice. And from there on out,
18 this consent signal is available. So in theory, any
19 third-party software, like analytics or advertising,
20 that loads after the signal is available can
21 potentially honor the user's opt-out request. The
22 data is there if they are able to get it, read it,
23 and act on it. But if all of that third-party
24 analytics and tracking and advertising code loads
25 before the consent manager, it's actually very hard,

1 in some cases impossible, for them to comply. The
2 information they need for compliance just isn't
3 there. So this is a real problem for users.

4 There's a number of different ways that
5 personal data gets shared and sold. As soon as your
6 browser starts sending HTTP requests to different
7 third parties, right off the bat, information that is
8 sensitive is almost certainly getting shared with
9 them. Every one of those HTTP requests can include
10 cookies that include pseudonymous identifiers. Other
11 personal data can be included as well. Once your
12 browser has finished contacting those third parties,
13 they can start executing JavaScript in the browser,
14 they can read and set more cookies, they can compute
15 probabilistic fingerprints. They're also able to do
16 things like scrape personal data out of the web page.
17 So, increasingly, third parties will look for things
18 like your email address or a phone number, and
19 they'll use that to construct a pseudonymous
20 identifier that is stable.

21 The previous speaker was talking about
22 things like identifier matching, cookie syncing.
23 That happens automatically as soon as the third
24 parties start to load. So it's not just one party,
25 but now multiple parties who all get this information

1 and are synchronizing it. I mean, basically, once
2 you have a third party loaded in a scenario like
3 this, all bets are off. The data is shared and sold.

4 So how does GPC help alleviate these
5 kinds of timing problems? Because GPC exists in the
6 user agent itself, in your browser, it's available
7 immediately from the moment the page begins to load.
8 By the time that your browser is getting HTML and
9 parsing it, GPC is already available. It's actually
10 already been sent to the publisher. It's very easy
11 now for the publisher, in JavaScript, to check: Has
12 this person opted out via GPC? That is all the code
13 is required to check to see if someone has opted out.

14 From there on out, the publisher can act
15 accordingly. One option is to just not load ad tech
16 at all. Another viable option is to continue loading
17 analytics and advertising, but to put it in a
18 restricted service provider mode by sending specific
19 parameters to them. So GPC is very helpful in this
20 regard. There's no waiting around for this signal,
21 it's just there all the time.

22 So the other problem I want to highlight
23 is this question of signal ambiguity. Coming back to
24 the consent management software, you have a website,
25 it's showing this banner, the user clicks the button,

1 they say they want to opt-out. That information,
2 that the person opted out, has to be distributed to
3 third parties so that they can act on it
4 appropriately. You click, and that signal needs to
5 go out somehow to everybody else. The problem is how
6 to do that.

7 Different consent managers and different
8 implementations try to distribute this consent
9 information in different ways. Sometimes it's placed
10 in a cookie or in something like local storage in the
11 browser, and the expectation is that third-party code
12 will just be able to find it and read it. Many of
13 the consent management platforms have their own
14 bespoke APIs. And there's not just one consent
15 manager, there are many of them, and their APIs are
16 different. The Interactive Advertising Bureau, they
17 have their own APIs that they've tried to standardize
18 across the industry. But they have at least two, and
19 their APIs are complex and not particularly well
20 adopted.

21 So if you're a well-meaning third party,
22 you are in sort of a pickle. You've been loaded into
23 a website. You would like to comply by reading the
24 consent information, but where is it? It could be
25 any of these places. So GPC also helps solve this

1 problem. GPC is one simple standard API. There's no
2 need to go hunting around for cookies or weird
3 consent manager APIs. Every HTTP request coming out
4 of the browser should include the GPC header, so
5 you're being told explicitly GPC is enabled. Or you
6 can look for the navigator object in the DOM, in
7 JavaScript, and just check, has the user made a
8 choice one API. No ambiguity.

9 So one of the things that we've been
10 doing lately is actually looking to see if third
11 parties are using the GPC APIs, and it turns out they
12 are. So we see at least 223 different third parties
13 calling the GPC APIs in the browser. 101 of them are
14 exclusively using the GPC API. We don't ever see
15 them trying to contact the consent manager or use the
16 IAB APIs. They just go directly to GPC. The other
17 122 use GPC and other APIs, so they're taking sort of
18 a multifaceted approach. But this is really nice to
19 see, that these third parties are already a little
20 bit ahead of the curve, in my opinion, and trying to
21 comply proactively.

22 So just to wrap up, it's my belief that
23 GPC is crucial for the success of the CCPA in
24 California. It ameliorates a lot of these technical
25 problems. "When is the signal available?" Well,

1 with GPC it's just available all the time,
2 immediately. And "where is the signal?" Well, GPC
3 just has the one simple API, so there's not a lot of
4 ambiguity.

5 I'll also highlight that I really believe
6 the browser, or the operating system, is the right
7 place for this functionality to be built. Because
8 that is the right place to implement the user
9 interface. There's no need to find and navigate a
10 million banners. You can make this choice once and
11 it becomes available everywhere. With consent
12 banners, if you clear your cookies, all of a sudden
13 your choices are lost, but that's not true with
14 something like GPC. And of course, there's no dark
15 patterns here. When this is implemented by your
16 browser, there's no incentive to try to manipulate
17 users. So, there's just a lot to really like about
18 GPC.

19 With that, I will conclude. I thank the
20 Board very much, and I am happy to take questions.

21 CHAIR URBAN: Thank you very much,
22 Dr. Wilson. Again, a really edifying and helpful
23 presentation, which I'm sure I speak for everyone in
24 saying that we appreciate it greatly. I think we do
25 have some questions for you, and we'll start with

1 Board Member Liebert.

2 MR. LIEBERT: Thank you for that great
3 presentation. How does the -- what appears to be the
4 evolving world towards an agentic AI marketplace, if
5 you will, in the ad context, how does that, if at
6 all, change your thinking about this and how we can
7 be most successful? Because it sure seems that's the
8 direction we're headed; correct?

9 DR. WILSON: Yeah. I mean, so I think
10 GPC helps in this regard as well. You know, the fact
11 that it's easier for a person to manage their
12 preferences and distribute them also makes it easier
13 for agents to distribute those preferences. I can
14 give the agent the preference and it can continue to
15 promulgate it. You know, there have been studies
16 where people try to get agents to do things like
17 click on banners for them. And it kind of works, but
18 it falls into the same traps as a person trying to
19 interact with those systems; right? Let's just
20 eliminate the ambiguity. You know, part of the
21 beauty of agents is that they automate things. GPC
22 is also about automation and standardization. So in
23 my opinion, they work together really well.

24 CHAIR URBAN: Thank you.

25 Other questions?

1 Board Member Ozer, please.

2 MS. OZER: I just have a question about
3 both sort of the scope of where GPC is currently
4 available for use. And also from a technical
5 standpoint, how is GPC sort of different in how it
6 functions or how it's available from something like
7 Privacy Badger or sort of other browser extensions.

8 DR. WILSON: Yeah. So I'll take that in
9 two parts. Thanks to the new law in California, GPC
10 should be included in all major web browsers version.
11 So that is awesome. There is some ambiguity there,
12 and I don't know how the law or the regs are going to
13 deal with this. But it is often true that apps will
14 embed browsers, and this is often done to display
15 advertisements. And this is kind of a weird
16 scenario. This is not Chrome or Brave or Firefox on
17 your desktop. This is now just an, an invisible
18 window within an app that's using browser technology,
19 but without any of the buttons, the menus, the
20 interface, none of that. So it is not entirely clear
21 to me how a user is supposed to express a GPC signal
22 in an embedded browser context like that.

23 This gets to kind of the second point,
24 which is mobile operating systems. I don't think
25 there's any requirement yet that Android or IOS or

1 any of the big mobile operating systems to adopt GPC
2 unilaterally. That is not good in my opinion. I
3 mean, the vast majority of web browsing is now done
4 on mobile devices. So when a person is on their
5 phone in a web browser, they will have this right.
6 But when they're on their phone in an app, they won't
7 necessarily be protected in the same way. Sebastian
8 also mentions this. You know, there are kind of self
9 regulatory regimes around the ad IDs on the mobile
10 devices, but that is not a substitute for actual
11 regulation.

12 You know, the other context I will
13 highlight is devices. So there's now a whole bunch
14 of studies looking at, you know, voice assistants
15 like Amazon, Alexis, smart TVs. We have a new study
16 coming out in a couple of months looking at connected
17 cars. They all include ad tech now. But it's not
18 browser based. So none of those devices are
19 necessarily going to have GPC, but yet they are still
20 collecting this information. So trying to extend
21 this kind of uniformity and simplicity of opt-out
22 into the device space, I think it's going to be
23 really important.

24 CHAIR URBAN: Thank you. Board Member
25 Ozer anticipated my question a bit as well. This is

1 Jennifer Urban. I was going to ask you to expand, if
2 you felt comfortable and could, on the mention you
3 made near the very end of your presentation, of
4 operating systems and browsers. And then you spoke
5 of browsers. And I understand from the examples that
6 you're giving now that in the mobile space, for
7 example, the browser may not be sufficient, in your
8 view. Do you have a view on signals and operating
9 systems more generally? And could you expand on that
10 for us?

11 DR. WILSON: Yeah. So I do think it is
12 important for operating systems to start adopting
13 universal opt-out technology. I mean, to a large
14 extent, I think Apple has led the way on this. You
15 know, any app that wants to do tracking has to ask
16 for permission. You know, that's largely enforced
17 either technically by preventing access to
18 identifiers by the OS, as well as by app store
19 policy. So if you continue to do things, and you
20 sell and share data, then you risk being delisted. I
21 think that's a pretty strong model. I would love to
22 see that turned into more affirmative regulation for
23 all the operating -- in all the major operating
24 systems.

25 CHAIR URBAN: Thank you. Any additional

1 questions or comments?

2 Okay. Thank you so much, Dr. Wilson.
3 And as with the other speakers, you're most welcome
4 to say. Ms. Schesser is going to be speaking next,
5 and then we will have public comments. And of
6 course, if you can't stay, we completely understand.
7 And all of the public comment will be available in
8 recording in a transcript for you. Thank you again
9 very much for that very helpful presentation.

10 Please bear with us for a few minutes
11 while we get set up for our next speaker, and then I
12 will introduce her.

13 All right. Our final presenter for this
14 information session is Ms. Stacy Schesser,
15 supervising deputy attorney general for the privacy
16 unit in the consumer protection section of the office
17 of the California Attorney General. Supervising
18 Deputy Attorney General Schesser leads the team that
19 enforces the CCPA at the California Attorney
20 General's Office. She began her career at the
21 attorney general's office in 2007 in its criminal
22 division and has worked in the privacy unit since its
23 inception in 2012. In 2014, she was named the
24 California privacy lawyer of the year.

25 And in -- what. I'm just reading what I

1 got.

2 So in 2024, she was named -- which I
3 was -- probably my typo. So we'll -- I'll be honest.
4 She was named California Privacy Lawyer of the Year.
5 And in 2019, was recognized as one of the Recorder's
6 Women Leaders in Tech Law, the only public sector
7 recipient of this award. So we are just replete with
8 award winning attorneys from whom to learn today.

9 Today, Ms. Schesser will highlight the
10 California Attorney General's enforcement of the
11 CCPA's opt-out preference signal requirements,
12 focusing on lessons learned from recent
13 investigations. She will also cover the Attorney
14 General's settlements involving the Global Privacy
15 Control, related agency enforcement actions, and
16 coordinated enforcement efforts with other attorneys
17 general.

18 Welcome Ms. Schesser. And please begin
19 when you're ready.

20 MS. SCHESSER: Thank you. Good
21 afternoon, Chair Urban, Board Members Ozer, Hamer,
22 and Liebert, Executive Director Kemp, and the
23 outstanding staff of Cal Privacy, and members of the
24 public. As Chair Urban said, my name is Stacy
25 Schesser. It's my honor to be here to speak to you

1 today. I have the privilege of leading a team of
2 exceptional attorneys on the privacy enforcement team
3 at DOJ, a role I've held since 2016. I am sharing my
4 views only, and they should not be attributed to the
5 attorney general. My remarks are limited to our
6 public enforcement actions, and I have to be mindful
7 about the confidentiality of our current
8 investigations.

9 With that said, I'm honored to speak to
10 you today about the hallmark of the CCPA, the
11 consumer's right to opt-out, and the expression of
12 that right via opt-out preference signal. This to me
13 is the most important aspect of the CCPA, and the
14 most critical one to think about being intentional,
15 broad, and protective of the consumer's right to stop
16 the proliferation of their data in the online
17 ecosystem and marketplace.

18 The GPC -- as speakers here today have
19 been very inspiring and very comprehensive in how
20 they've explained it. GPC uses existing web
21 infrastructure and technologies to solve many of the
22 timing and technical challenges presented by ad tech
23 and the data industry that instantly and invisibly
24 sell and share consumers' personal information. It
25 is an incredibly important tool that gives the

1 consumer the power to automate privacy with the same
2 force and pervasiveness as those seeking to monetize
3 data. It also expresses one powerful sentiment:
4 Stop. Stop selling my data. Stop sharing it for the
5 purposes of cross-contextual behavioral advertising.
6 Stop trading it with third parties. Stop giving it
7 to data brokers. Stop tracking me. Just stop.

8 But I would like to provide some
9 background as to when we first wrote the initial
10 regulations establishing a user-enabled Global
11 Privacy Control. We wrote the language to be as
12 intentional as possible, with every word having
13 meaning. And these words include "the consumer if
14 known," and it was developed in consultation with our
15 long-standing brilliant contract technologist Nathan
16 Good. It was solidified in our Disney enforcement
17 action, recently filed in February 2026, which
18 Mr. Goldberg discussed and I'm going to discuss a
19 little bit more at length in a few moments.

20 We also understood, and continue to
21 enforce, this right to be one that is broad,
22 investigating its implementation and effectuation to
23 include downstream entities, and conceptualized it as
24 a persistent privacy choice. A consumer sets it and
25 forgets it, and even one that could be expressed by a

1 consumer who chose a privacy product that built GPC
2 in by default. And finally, we wanted to mandate
3 that user-enabled Global Privacy Control is one
4 that's deeply protective of the right to opt-out.

5 Originally, a consumer would have to
6 click the "do not sell my personal information" link
7 on every website, on every browser, and every device.
8 But with the regulations enshrining the right to
9 opt-out via a user-enabled Global Privacy Control,
10 the mechanism by which a user expresses this right
11 became global and persistent, all while reducing
12 burden on the consumer. When GPC was introduced, it
13 was supposed to be as easy, immediate, and pervasive
14 as ad tech. It's supposed to be a constant signal
15 that interrupts the system of real-time bidding an
16 average consumer has no idea happens in the
17 background and in microseconds when they land on a
18 website page. And while GPC is currently only
19 available on web browsers, the law requires that a
20 business applies a consumer's opt-out to that
21 consumer, and thus to apps running on their phone, to
22 smart TVs, and other connected devices. Again
23 intentional, broad, protective.

24 While the GPC is an amazing tool to
25 protect consumers, it succeeds because it has legal

1 teeth behind it. But even the best law on paper is
2 nothing without robust enforcement. And it is
3 because of our offices, DOJ, and Cal Privacy's
4 consistent and rigorous enforcement of these
5 requirements that GPC and consumers' CCPA rights have
6 meaning and impact. We take consumer privacy very
7 seriously.

8 And I also want to note that it went from
9 a concept that was in regulation, and informed much
10 to be the product based on input that was from
11 academics, much like today's session, to drive
12 enforcement. And today, as I'm sitting here and
13 listening, I also want to say it's provided a good
14 deal of inspiration for future-looking enforcement.
15 But today, I'm going to discuss three enforcement
16 actions that cement important takeaways that we want
17 businesses to understand for compliance.

18 And so there's three major themes that
19 I'm going to discuss. Number one, that businesses
20 are required to accept and process the GPC. Number
21 two, that they are required to ensure that GPC is
22 technically implemented correctly. And number three,
23 that when you apply GPC requests, they are applied to
24 the consumer, and not just the individual devices or
25 browsers where the signal is detected. Before I dive

1 into these actions, I want to emphasize the
2 enforcement of GPC is an ongoing priority for DOJ and
3 has been from its inception. On the first day that
4 CCPA became enforceable, July 1st, 2020, we sent
5 letters out. We hit the ground running hard. After
6 the regulations became final, GPC was referenced by
7 then Attorney General Xavier Becerra on Data Privacy
8 Day in 2021, when he said, and quote, "CCPA opened
9 the door to developing a technical standard like the
10 GPC, which satisfies the legal requirement and
11 protects privacy."

12 We've also conducted several sweeps that
13 investigate how companies are complying with CCPA's
14 requirements, and we always double check for the GPC.
15 Now when we conduct sweeps, the regulated community
16 pays attention. They conform their practices so that
17 when we do come knocking and take a look under the
18 hood, they are solid on some of the areas that we
19 have swept in previous investigations. This is a
20 good thing. We want businesses to comply, and we
21 want to hear that when we find issues, they are on
22 it, and that they are on it quickly. That is the
23 type of response that we expect as enforcers and
24 consider when exercising our discretion. But it is
25 our filed actions, and in particular our complaints

1 and judgments, that has best communicated to the
2 industry how we enforce GPC to ensure Californians'
3 maximum protection of their opt-out rights.

4 Our first action involving GPC was in
5 August 2022 and involved Sephora, led by
6 now-supervising Deputy Attorney General Ronnie
7 Pomerantz. Sephora came about as part of a 2021
8 enforcement sweep investigating how large retailers
9 sell personal information and how they are responding
10 to a consumer signaling their opt-out via the GPC.
11 We specifically articulated how we tested whether
12 traffic changed after enabling the GPC, finding that
13 in Sephora's case, data continued to flow to
14 third-party companies, including advertising and
15 analytics providers. In operating its online website
16 and selling products, Sephora collected and amassed
17 information about consumers, including the products
18 that consumers view and purchase, their geolocation
19 data, cookies, and other user identifiers, and
20 technical information about operating systems and
21 browser types.

22 At first blush, Sephora disclosed in its
23 privacy policy that it shared consumers' geolocation
24 and internet or other electronic network activities
25 with third parties, including ad networks, business

1 partners, data analytic providers, and others. But
2 it did not offer the right to opt-out, even though
3 Sephora made this data available to these companies
4 by installing or permitting the installation of
5 third-party tracking technologies, including cookies,
6 pixels, SDKs, and other technologies, and they did so
7 in return for advertising or analytic services. In
8 return, Sephora knew that it would receive discounted
9 or higher-quality analytics and other services
10 derived from the data about consumers' online
11 activities, including the option to later target an
12 advertisement to consumers that had merely browsed
13 for their products online. Yet, when a California
14 consumer signaled their opt-out using the GPC,
15 nothing changed to block or flag the transmission of
16 personal information.

17 In short, they completely ignored the
18 GPC. After receiving a notice from the attorney
19 general alleging that it had sold consumer data
20 without offering the right to opt-out, Sephora failed
21 to cure these violations within 30 days, at the time
22 when there was a cure period in effect. And in our
23 settlement, we negotiated with the company that it
24 would be bound to comply with the law, and
25 specifically mandated that it process consumer

1 requests to opt-outs signaled via a GPC.

2 I also want to highlight another case,
3 Healthline, led by Deputy Attorney General Mike
4 Osgood. Healthline offers many takeaways to the
5 industry, but it was an important opportunity that
6 the attorney general described why GPC is so
7 important for consumers. Specifically, our complaint
8 stated, "Because the online trackers used to
9 facilitate cross-contextual behavioral advertising
10 operate invisibly, ubiquitously, and nearly
11 instantaneously in the background of web pages, the
12 GPC meets this challenge by operating invisibly and
13 continually in the background to tell each business's
14 website that the consumer is opting out." In
15 Healthline, even for a consumer who had triple opted
16 out via a do-not-sell link, clicking reject in the
17 cookie banner, and transmitting the GPC, Healthline
18 continued to sell personal information to third
19 parties for online advertising.

20 Unlike Sephora, Healthline had
21 implemented a response to the GPC. But it had done
22 so incorrectly. Not properly configuring their
23 software tools to recognize GPC, not doing auditing
24 or testing, and continuing to do so, is an actionable
25 violation. And that's what Healthline importantly

1 stood for. When businesses choose to implement
2 complex technologies to sell and share consumer data,
3 it is the business's obligation to ensure GPC stops
4 selling. It is only a set-it-and-forget-it for
5 consumers, it is not for businesses. Because after
6 all, these are rights as determined by our
7 legislature and later affirmed by the electorate.

8 Finally, I want to walk through our most
9 recent enforcement action, that we've already
10 discussed a little bit today, in Disney, which was
11 filed in February 2026, led by Deputy Attorney
12 General Maneesh Sharma. As with each of our
13 enforcement actions, we sought to make something
14 crystal clear, and that is that opt-outs, including
15 by the GPC, apply to the person, not the devices. We
16 are, after all, enforcing the California Consumer
17 Privacy Act, not the California Device Privacy Act.
18 Our investigation into Disney was part of an annual
19 Data Privacy Day investigative sweep during the year
20 that we focused on streaming.

21 Disney streaming services required that a
22 consumer have an account and log in before watching
23 content. This meant that each time a consumer
24 watched a movie, a show, or a sporting event, Disney
25 knew who was watching, and the gadgets and gizmos

1 aplenty that they used, whether it was a connected
2 TV, laptop, cell phone, or tablet. Disney leveraged
3 their ability to identify consumers across devices
4 into a profitable advertising business by touting its
5 ability to deliver targeted ads across services and
6 devices to the consumer. But while Disney and
7 similar companies are able to instantly deliver
8 targeted ads to the many connected devices we use, we
9 found that they did not push out and implement a
10 consumer's opt-out across those same devices. It
11 underscored that there's a disconnect between how
12 industry has approached privacy compliance as opposed
13 to how they've built their data collection and
14 monetization systems.

15 For decades, companies have been
16 implementing and relying on a web-focused consent
17 model that relies on cookies and other non-persistent
18 tools that is often limited to a single device or
19 browser. As a result, consumers face a never-ending
20 story of consent pop-ups and cookie banners, and are
21 even told that their opt-out requests will have to be
22 resubmitted if they clear cookies. In contrast, on
23 the data side, industry has massively invested in an
24 identity-based model that allows businesses to
25 quickly track, combine, and monetize consumer data

1 collected across various devices, and locate a
2 specific consumer on their specific device to show
3 them a perfectly targeted ad or message. And despite
4 the business community claiming commitment to
5 privacy-by-design principles, our enforcement
6 investigations have shown that these identity-based
7 tools were not designed to properly integrate with
8 companies' existing privacy compliance tools. With
9 our enforcement action in Disney, we were able to
10 reinforce that the CCPA and privacy compliance
11 entered a whole new world. That's the last one.

12 When businesses can associate a
13 consumer's device for advertising purposes, they can
14 and they must associate those devices to honor that
15 consumer's opt-out. We were able to emphasize that
16 the CCPA does not permit a business to limit the
17 GPC's reach to only web browsers where GPC is
18 currently available. Since CCPA went into effect,
19 and with the very first iteration of the CCPA
20 regulations and in every rulemaking that followed,
21 our technologists and Cal Privacy experts have
22 recognized that businesses have multiple ways of
23 identifying consumers across the web, and require
24 that GPC be treated as a valid request to opt-out if
25 known and for the consumer. This requirement means

1 that once a company has connected any device to a
2 consumer's identity, whether pseudonymous or not, the
3 business is obligated to opt-out that identity,
4 including all devices associated with the identity.
5 This requirement is important to ensure that an
6 opt-out preference signal meets the goal of being a
7 simple, single step to opt-out, whether across
8 multiple businesses or within one large business.

9 Ensuring that the opt-out preference
10 signal applies to consumers is especially relevant,
11 because consumers are constantly interacting with
12 businesses online through their computers, but also
13 phones, tablets, and connected TVs, and we heard from
14 Dr. Wilson now their cars, where GPC is not currently
15 available. Notably, Disney is not unique in having
16 multiple touch points with consumers, and in relying
17 on a privacy compliance technology that no longer
18 matches how companies sell, share, and use consumer
19 data. We have heard over and over that off-the-shelf
20 vendor technology is not keeping pace with the
21 requirements of the CCPA, and that real compliance
22 requires customized solutions. But businesses that
23 have the resources to update their data monetization
24 structure must also invest in resources to match
25 privacy compliance, so consumers can easily stop all

1 sales and sharing of their data without having to
2 individually opt-out with multiple businesses and
3 multiple devices.

4 In addition to Sephora, Healthline, and
5 Disney, and as I'm sure you're well aware, GPC is
6 being robustly enforced by Cal Privacy as ratified in
7 recent settlements with Tractor Supply and PlayOn,
8 where businesses failed to recognize and honor
9 opt-out preference signals on their web properties.
10 And we applaud Cal Privacy's extensive enforcement
11 work there as well. I would also like to point out
12 that even though my remarks today are about companies
13 that did not comply with GPC, we are seeing companies
14 who are endeavoring towards compliance. Companies
15 are integrating and updating their systems for GPC
16 even as we continue to maintain pressure through
17 enforcement. We should continue to maintain that
18 pressure on developing GPC for mobile and
19 beyond-browser integration.

20 Indeed, it is exciting that we will soon
21 enforce new requirements set forth in AB566,
22 requiring companies to build in opt-out preference
23 signal functionality within their browser, thanks to
24 the Agency's stellar legislative advocacy and the
25 work of Maureen Mahoney. Mobile devices and the very

1 sensitive data that comes along with them need to
2 develop better tools for consumers and for opt-out
3 preference signals. While both Android and iPhone
4 provide controls to delete ad IDs or request apps not
5 to track, ad tech companies regularly attempt to
6 circumvent them to continue tracking users.

7 Consumers want and need robust and comprehensive
8 privacy solutions, and I say this with deep
9 appreciation that I'm speaking during the first week
10 in which data brokers will begin processing requests
11 via DROP.

12 Please continue to keep opt-out
13 preference signals the robust tool that it is. I
14 caution the Board about considering adding more
15 language to the regulatory text, as it could allow
16 companies the opportunity to sometimes blur the line
17 for compliance. Continued enforcement will
18 effectively telegraph the requirements of the law for
19 businesses that fail to fully effectuate a consumer's
20 right under the CCPA.

21 I want to close with noting that
22 California sets the standard for the rest of the
23 country. As former Attorney General Kamala Harris
24 said, "As California goes, so goes the nation." It
25 is because of our innovation here, both legal and

1 technological, that consumers enjoy robust privacy
2 protections. It is because of our standards and
3 demands for better privacy rights that states are now
4 following in our footsteps, with many more states
5 providing rights for their own constituents to
6 exercise their rights via opt-out preference signals.
7 I have found also, in reviewing federal privacy laws
8 and federal privacy bills, that Congress has included
9 references to opt-out preference signals, but has
10 erroneously required further study or pausing its
11 immediate effect language that we should continue to
12 oppose. Because GPC is working, and it will continue
13 to work in California, as it has for over six years
14 now. Please continue to support opt-out preference
15 signals as a robust tool for consumers, and I will
16 continue to do my job to enforce the law so that this
17 tool only becomes stronger, even more protective,
18 intentional, and broad for consumers. Thank you.

19 CHAIR URBAN: Thank you. Thank you very
20 much, Ms. Schesser. And of course, the Board and the
21 Agency greatly appreciate all of the attorney
22 general's leadership in this space as well. And we
23 have been very pleased to see the cooperation that
24 the two agencies have undertaken with regards to
25 enforcement. Which is, as you say, more guidance for

1 businesses. As we publish enforcement actions. I
2 have -- I'm going to ask you if you have views that
3 you think would be helpful to the Board when it comes
4 to regulations or other guidance that would be
5 responsive to Mr. Goldberg's question?

6 So I heard you loud and clear. Privacy
7 protects people, not devices. And if somebody is
8 known, even if they're pseudonymous, then the GPC
9 signal should propagate and should be respected. Do
10 you have views on the probabilistic identifier
11 challenge that Mr. Goldberg identified for us or
12 described for us? If there is a mushy middle, or you
13 don't think there is a mushy middle, or if there's a
14 mushy middle, if there's something that you think
15 that we could do to make that easily actionable.

16 MS. SCHESSER: I don't have specific
17 views. And I heard the complexity of that question
18 that you had asked Mr. Goldberg, which I thought he
19 tried to answer as -- you know, as best as he could,
20 given the complexity of the question. The only thing
21 I will say is that when thinking about these things,
22 you know, I don't want to speak too much because this
23 may be something that could come up in the context of
24 enforcement. It could come up in the context of an
25 investigation, and it could be something that, based

1 on how companies are responding to opt-outs, could
2 even go beyond CCPA and, you know, potentially become
3 an unfair business practice, something that is
4 deceptive as well. And so I want to be very careful
5 about, you know, speaking specifically on potential
6 text or regulation that targets that, because it
7 could also be something that we interpret through the
8 lens of enforcement.

9 CHAIR URBAN: Absolutely. Yes. All
10 right. Thank you very much.

11 Are there questions or comments from
12 other board members?

13 Board Member Hamer?

14 MS. HAMER: Yeah. No. You actually said
15 what I was going to say, so thank you for that. But
16 thank you for your work. It is a really interesting
17 overview. Appreciate it.

18 CHAIR URBAN: Thank you.

19 Board member Liebert?

20 MR. LIEBERT: Yes. You are a legend in
21 the privacy world. I thank you for all your great
22 work. It sure seems like we're on the precipice of a
23 true revolution in the ad tech world when it comes to
24 the evolution now of AI and AI platform and what
25 they're signaling, that those two are going to be the

1 means by which we are targeted with advertisements
2 and given advertisements. And I'm wondering to what
3 extent now the GPC world needs to evolve in that
4 regard because right now, of course, they're not, I
5 believe, covered by the law in regards to that
6 process. So to what extent are, are we going to face
7 those issues?

8 MS. SCHESSER: I will just say that while
9 the conversation was happening, I was scribbling
10 notes and having different thoughts, and I would like
11 to just reserve the ability to continue to think
12 about that and how it would apply in the context of
13 CCPA.

14 CHAIR URBAN: All right, Counsel. You
15 can reserve your time, and we'll bring you back for
16 another session.

17 Other comments or questions from the
18 Board?

19 Thank you again, Ms. Schesser. Fantastic
20 presentation. I very much appreciate it.

21 That concludes the informational session
22 presentation to the Board. And I would like to
23 welcome public comments on any of the topics that we
24 have discussed so far today through the presentation.
25 If there's anyone here in person who would like to

1 make public comment, please proceed to the podium,
2 and I will call on you when ready.

3 And if there's anyone on Zoom who would
4 like to make public comment, please raise your hand
5 using the raise your hand function in your Zoom
6 application, if you're using that. If you are using
7 your phone to call into the Zoom, I believe it is
8 star-six to raise your hand. And I am going to check
9 with Ms. Carwile to be sure I got that right.

10 Star-nine. I flipped it. Okay. Apologies to
11 everybody on zoom by phone. If you would like to
12 make a public comment, please press star-nine. And
13 Ms. Carwile will call on Zoom participants when we
14 are ready and unmute them. And then she will mute
15 you again when you are done.

16 For folks in the room, I will ask you to
17 speak into the microphone for purposes of the record.
18 And we will start with our first comment in the room.
19 As a reminder, you have three minutes. Thank you
20 very much.

21 MR. KATHLACABE: Thank you. My name is
22 Mike Kathlacabe, and I'm here in my personal capacity
23 as a consumer in California.

24 So first, let me say that I'm glad I live
25 in California where we have a California Privacy

1 Protection Agency, and we have a California
2 Department of Justice that actually enforces the
3 rules. On the other hand, I see the efforts to
4 protect privacy relying on opt-out as kind of a game
5 of wack-a-mole; right? Advertisers and the market of
6 surveillance capitalism is constantly trying to find
7 ways around the protections that we put in place. It
8 shouldn't be incumbent on the consumer to opt-out of
9 all of the various things in order to protect their
10 privacy. It should be opt-in.

11 Now, I realize you're working with the
12 law as it exists and perhaps not as we would like.
13 So that's incumbent upon me as a consumer and a voter
14 in California to try to change that law. But one of
15 the things as a consumer and obtaining information
16 about myself from data brokers is realizing that as
17 someone who is very interested in privacy, I take all
18 of the measures I can to protect my privacy. And yet
19 when I get reports about myself from data brokers, I
20 am amazed that they are able to tie my physical
21 credit card transactions to my online persona and
22 multiple email addresses. And again, like I said,
23 I'm using all the privacy browser settings. I'm
24 using privacy add-ons. I'm using ad blockers, all of
25 those things. But even for me -- and I consider

1 myself relatively sophisticated when it comes to
2 protecting my privacy -- it's a game of wack-a-mole
3 for me, and I'm not successful. Please keep this in
4 mind in going forward.

5 And Department of Justice, keep on doing
6 your thing. It would be great if instead of settling
7 with some of these companies, we could actually cause
8 actual consequences for them. I know you can't put a
9 company in jail yet, but just allowing them to pay
10 their way out of violating our privacy doesn't seem
11 like an adequate solution. So once again, thank you
12 for this. I very much appreciate it. And good luck,
13 because I think we all need it.

14 CHAIR URBAN: Thank you so much. We
15 really appreciate the public comments and you joining
16 us today in person. Are there any other public
17 comments here or on Zoom?

18 MS. CARWILE: Yes, we do have somebody on
19 zoom, and that's Ben Tobin. I'm going to unmute you
20 at this time. You'll have three minutes to make your
21 comments. So please begin when you are ready.

22 MR. TOBIN: Oh, I had to hit the button.
23 Good afternoon, Chair Urban, Board Members Hamer,
24 Liebert, Mactaggart, Ozer, and Executive Director
25 Kemp. My name is Ben Tobin. I run Surveil, a

1 California company.

2 So what do we do? We search the index
3 internet, including data broker sites, to verify
4 whether a person's information's exposed online. And
5 I do have a commercial interest in this. No one has
6 sent me, and I am speaking for myself. I'm here to
7 address recommendations one and two. And I think
8 there's somewhat of the same problem. And I'll start
9 with something in your own regulation.

10 So specifically, Section 7022, that's
11 7022, says, "A business complies with the request to
12 delete by erasing the information or de-identifying
13 it or aggregating it." And this is kind of the
14 kicker, the business gets to choose. And it only has
15 to notify the consumer whether it complied and not
16 which action it took. So let's say me, the consumer,
17 asked to be deleted. I'm told "yes," but I never
18 actually learn which of the three options were
19 executed.

20 And then I kind of want to drive home on
21 the third one, aggregation in this kind of agentic AI
22 model building space that we're dealing with now.
23 Aggregation is not technically a destruction. It's a
24 change of form. The information is technically gone
25 as a record, but it's present as a training set. And

1 a training set can still produce actionable insights
2 about the person that it came from, whether ever
3 needing that person's name again. That is
4 recommendation to a profile that acts on someone
5 without having to identify them. The deletion is
6 real. The compliance is real, and nothing really
7 about that person's exposure has changed.

8 Now, what we're doing is we're kind of
9 introducing friction here through the CCPA. And in a
10 world with a fixed appetite where data brokers are
11 concerned, that would be appropriate. However, data
12 that becomes a model never really decays, and it
13 doesn't have to be reacquired. It can basically just
14 sit around until it's used, these models, and then
15 produce results. And now, I do want to be careful
16 here. I'm not saying anyone's actively doing this,
17 but what I am saying is that your own rules do permit
18 it and nothing actively requires anyone to disclose
19 it, and nothing technically would show it.

20 So the words I suggest should carry more
21 weight. Opt-out should mean you do not get to watch
22 me and delete me should mean just that. Delete me.
23 And on recommendation one, your own rule already
24 knows this. Section 7025 promises a consumer can
25 opt-out with all businesses, but it then adds four

1 words, "they interact with online." Those four words
2 at the end of a sentence, nobody outside of this room
3 necessarily has read. The consumer hears all
4 businesses, but the rule means the ones whose
5 websites they've opened.

6 MS. CARWILE: Thank you. That is three
7 minutes.

8 MR. TOBIN: Have a good day. Thank you
9 for your time.

10 MS. CARWILE: If there are any other
11 members of the public who'd like to speak at this
12 time, please go ahead by using the raised hand
13 feature or by using star-nine if you're joining us by
14 phone. Again, this is for Agenda Item 2.

15 Madam Chair, I'm not seeing any other
16 hands raised at this time.

17 CHAIR URBAN: Thank you very much. And
18 thank you for the public comment that we received on
19 Zoom as well.

20 Before we move to the next agenda item,
21 we are going to take a break of about 15 minutes.
22 It's 10 or 15 minutes. Let's come back at 3:30. Is
23 that sufficient for everybody's purposes? Okay.
24 Wonderful. So we will come back at 3:30, for those
25 of you on Zoom. And thanks again to our speakers and

1 to everyone for their attention, questions and
2 comments.

3 (Whereupon, a short recess was
4 taken.)

5 CHAIR URBAN: Welcome back, everyone.
6 Thank you for giving us some time to take a break.
7 We will now turn to agenda Item Number 3, which is an
8 item on preliminary rulemaking update and
9 recommendations from staff on opt-out preference
10 signals. So we have been well prepared by the
11 discussion that we just had. It will be presented by
12 Philip Laird, the general counsel of CPPA, Lisa Kim,
13 senior privacy counsel and advisor to the Agency, and
14 Rianna Grenda, senior legal analyst, CPPA. I will
15 ask the team to please go ahead when you're ready and
16 everyone to turn to the materials in your packet for
17 this agenda item.

18 But I cannot let this moment pass without
19 mentioning that we have yet another recipient of the
20 California Lawyers Association Privacy Attorney of
21 the Year award in the form of Ms. Lisa Kim. So we
22 really are being advised by the best, and we are very
23 grateful for it. Please go ahead.

24 MR. LAIRD: Thank you, Chair Urban, and
25 members of the Board. And actually, to start with

1 that point, I'd love to note that, in fact, all four
2 recipients ever in the history of the Privacy Lawyer
3 of the Year award are in this room right now. So
4 we're very, very excited to have a full --

5 CHAIR URBAN: I'm getting the last one
6 tomorrow, so.

7 MR. LAIRD: Exactly. And furthermore, I
8 just want to take the opportunity to thank the
9 speakers this afternoon. We really appreciate them
10 to taking time out of their days to be with us to
11 present to the Board and staff and the public. I
12 found it very informative, and I hope you all did as
13 well.

14 CHAIR URBAN: Actually, we're going to
15 break protocol for a moment, because Board Member
16 Liebert would like to say something very quick.

17 MR. LIEBERT: Wow. Terrific program. We
18 all, as a board, decided together to pursue these
19 informational hearings where you're educating us
20 since you already understand all this. And thank you
21 so much. It was really a terrific program and
22 really, really appreciate how these are developing.
23 They're excellent.

24 MR. LAIRD: Well, thank you. And
25 complements certainly go to the two to my right, who

1 were very much behind thinking through who would be
2 the appropriate speakers to cover so much territory
3 and so much important work being done. So to begin,
4 as a reminder, at our November 2025 board meeting,
5 the Board directed staff to begin preliminary
6 rulemaking on four topic areas. One was opt-out
7 preference signals, another was reducing friction in
8 the exercise of privacy rights, a third was notices
9 and disclosures, and a fourth was employee data.
10 Just a few small topics.

11 Today we will provide a preliminary
12 rulemaking update, along with proposed rulemaking
13 recommendations related to the first topic, opt-out
14 preference signals. But to preview for the Board
15 today, we do plan to present updates to the Board on
16 our work on both reducing friction in the exercise of
17 privacy rights and notices and disclosures at the
18 Board's November meeting of this year, and we are
19 then planned in February to present our preliminary
20 rulemaking updates on employee data. So, the legal
21 division has been hard at work carrying out the
22 direction of this Board, and I'm pleased that we are
23 moving at a good pace, and plan to have these
24 presentations to you over the course of the next
25 several meetings.

1 That said, if the Board has any concerns
2 regarding the schedule, we of course welcome that
3 feedback. And with that all said, I will now turn to
4 the professionals to my right, senior privacy counsel
5 and adviser Lisa Kim and senior legal analyst Rianna
6 Grenda, who will walk you through today's preliminary
7 rulemaking update and proposed recommendations
8 related to opt-out preference signals.

9 MS. KIM: Great. Thank you so much. So
10 as mentioned, over the past 10 months our OOPS team,
11 our opt-out preference signal team, has been
12 diligently evaluating whether additional OOPS
13 regulations are necessary and would be beneficial to
14 businesses and consumers. So we appreciate the
15 opportunity to present our recommendations to the
16 Board today.

17 This afternoon we're going to walk you
18 through three items. First, we'll provide some
19 level-setting background on OOPS. Second, we'll
20 offer an overview of the preliminary rulemaking
21 activities our team has undertaken. And finally, we
22 will present our recommendations for the Board's
23 consideration. See if I can get our slide up.

24 That said, before we begin, I wanted to
25 acknowledge a team member who wasn't able to join us

1 today. Joe Brown, the Agency's former fellow,
2 contributed meaningfully to this work before
3 completing his fellowship and then moving on to
4 permanent employment. So I want to just do a little
5 shout-out. Joe, if you're watching, we just want to
6 acknowledge and thank you for your efforts and the
7 support you provided during this process.

8 So, starting with the background on
9 opt-out preference signals. The informational
10 session covered some of this, but we believe it's
11 important to understand the context of how OOPS came
12 about, as we talk about recommendations. As set
13 forth in the regulations, "The purpose of an opt-out
14 preference signal is to provide consumers with a
15 simple and easy-to-use method by which consumers
16 interacting with businesses online can automatically
17 exercise the right to opt-out of sale and sharing.
18 And through an opt-out preference signal, a consumer
19 can opt-out of the sale and sharing of their personal
20 information with all businesses they interact with
21 online, without having to make individual requests
22 with each business." So opt-out preference signals
23 align very well with our strategic goal of allowing
24 consumers to exercise their rights at scale and in a
25 simple and easy way.

1 Now, as Professor Zimmeck previewed
2 earlier, opt-out preference signals were part of the
3 very first iteration of the CCPA regulations well
4 before the CPRA came out, and also before the Agency
5 was created. In August 2020, the attorney general
6 adopted a forward-looking regulation to treat as a
7 valid request to opt-out a user-enabled Global
8 Privacy Control, such as a browser plug-in or privacy
9 setting, device setting, or other mechanism that
10 communicates or signals the consumer's choice.

11 In response to that regulation, a group
12 of privacy researchers, including Professor Zimmeck
13 and our former executive director Ashkan Soltani,
14 developed what became known as the Global Privacy
15 Control, which was later introduced at the World Wide
16 Web Consortium, W3C, in October 2020. A month later,
17 California voters voted on CPRA. In early 2021, the
18 attorney general publicly confirmed that GPC met the
19 CCPA's requirements for a user-enabled opt-out
20 mechanism. And then a year and a half later, in
21 August 2022, the AG announced its first CCPA
22 settlement, with Sephora, which included allegations
23 that Sephora had failed to honor GPC. Now, CPRA
24 amendments to the law went into effect shortly after
25 that, using the term OOPS instead of global privacy

1 controls.

2 And so, to clear up any confusion between
3 the CCPA regulations and the CPRA's new amendments to
4 the law, the Agency adopted regulations that
5 reiterated the requirements set forth in the original
6 CCPA regulations to ensure consistency between the
7 old and current regulations. After that, enforcement
8 of OOPS requirements and the GPC has continued
9 steadily by both the AG's office and Cal Privacy.
10 Healthline, Tractor Supply, PlayOn Sports, and most
11 recently Disney all involved businesses who failed to
12 honor GPC. And then most recently, the legislature
13 passed AB566, an Agency-sponsored bill requiring
14 browser developers to offer OOPS functionality. And
15 that law will go into effect in January 2027.

16 Now, I go through this background because
17 I believe it helps illustrate how OOPS has grown over
18 time, and it provides a helpful foundation for
19 understanding the preliminary rulemaking activities
20 we carried out next. And I'm going to turn the
21 presentation over to Rianna Grenda, the senior legal
22 analyst on our OOPS team, who will walk you through
23 those.

24 MS. GREND: Thank you, Lisa.

25 Good afternoon, members of the Board and

1 members of the public. I am going to walk us through
2 some of the work that our team has done up to this
3 point, work that has helped inform our
4 recommendations that we're going to go over later in
5 this presentation.

6 Part of our preliminary work included
7 stakeholder outreach. This included engagement with
8 our partners, including the Attorney General's
9 Office, our own enforcement team, as well as our
10 legislative division. We also drew on the expertise
11 of our technologists, who unpack the technically
12 complex parts of opt-out preference signals, or OOPS,
13 and we found their insights to be very valuable. We
14 also engaged with the business community, consumer
15 advocate organizations, as well as academics and
16 thought leaders. Overall, these conversations helped
17 us better understand operational realities with
18 opt-out preference signals and consumer protection
19 concerns.

20 In addition to stakeholder engagement, we
21 conducted our own research. We completed a
22 state-by-state survey of all adopted and pending
23 universal opt-out mechanism laws to identify trends,
24 common approaches, and areas of divergence. We also
25 reviewed a wide set of materials, including academic

1 studies, white papers, news reports, related
2 legislation, and we also closely examined the AG's
3 rulemaking package on SB976, the Protecting Our Kids
4 from Social Media Addiction Act, particularly the age
5 verification components.

6 Lastly, we did an in-depth review and
7 analysis of the comments that were submitted to us
8 during our preliminary written comment period. Which
9 brings me to the next couple of slides, where I will
10 briefly summarize the written comments that we
11 received. So we received 43 written comments,
12 totaling 376 pages. These comments related not only
13 to our team's work, but also the reducing friction
14 group's work. These commenters represented business
15 and trade organizations, consumers and consumer
16 advocate organizations, data brokers, authorized
17 agents, academics, and legal practitioners. The
18 diversity of this input really helped us identify
19 areas of alignment, areas of tension, and where
20 further clarification or direction may be needed as
21 we move toward rulemaking.

22 On this slide, you will see a high-level
23 summary of the themes that we saw across the written
24 comments. We received a wide variety of comments.
25 Some were very substantive, others were less relevant

1 to the rulemaking. For example, a few companies did
2 talk about their own privacy products, and some
3 commenters raised concerns about the underlying law
4 rather than the regulations themselves. But when we
5 filtered through all of the comment submissions,
6 there were a few themes that emerged, and those are
7 reflected here.

8 One major theme involved issues with
9 processing GPC, including how it applies to
10 pseudonymous profiles, known consumers, and
11 situations where GPC conflicts with a user's privacy
12 settings. Another recurring theme was timing issues,
13 such as when GPC interacts with the firing of
14 cookies. We also saw interest in recognizing
15 additional mechanisms or signals as OOPS. Some
16 commenters emphasized the need for
17 competition-neutral safeguards in applying OOPS
18 uniformly, which would largely require statutory
19 revisions to balance third-party versus first-party
20 data rights. There were also a few items that only
21 came from one or two commenters, such as AI handling
22 of GPC as well as age-signal interoperability. These
23 weren't widely raised, but they are worth noting as
24 emerging ideas that may become more prominent over
25 time. Overall, this feedback helped us identify

1 where stakeholders are aligned, where there's
2 confusion, and where additional clarity may be needed
3 as we develop regulations.

4 Okay, and now I'm going to go ahead and
5 hand this back to Lisa Kim, who will walk us through
6 the recommendations that we are considering.

7 MS. KIM: Okay. The fun part. Based
8 upon our work, staff have four recommendations for
9 the Board, and they are: First, explicitly
10 identifying GPC as an OOPS; number two, including
11 examples clarifying how OOPS applies to pseudonymous
12 profiles; third, requiring the reporting of OOPS
13 metrics; and four, including examples clarifying
14 timing issues regarding GPC and the sale and sharing
15 tracking technologies we see in the marketplace.

16 So I'll start with the first one,
17 explicitly identifying GPC. Our first recommendation
18 is that the Board explicitly identify GPC as an
19 example of an OOPS. As the history we covered
20 already shows, GPC has functioned as an OOPS since
21 the earliest iterations of the CCPA regulations. So
22 including GPC by name in the regulation would reflect
23 its established role over the years, while also
24 reinforcing existing enforcement standards and
25 supporting the ongoing work of the attorney general

1 as well as the enforcement division of Cal Privacy.
2 In addition, explicitly identifying GPC would help
3 support consistent implementation across states with
4 universal opt-out requirements. As you may know, 13
5 other states have passed legislation related to
6 universal opt-out mechanisms, and several of those
7 states include language requiring their own OOPS or
8 universal opt-out mechanisms to align with similar
9 tools that are recognized under other federal -- or
10 state laws. So for us to clarify in California
11 regulations that GPC is a valid OOPS would actually
12 make it easier for other states to recognize GPC as
13 meeting California's standard, and therefore
14 ultimately promote greater uniformity and reduce
15 compliance challenges throughout the country.

16 Our second recommendation is that the
17 Board consider adding examples illustrating how OOPS
18 applies to pseudonymous profiles. While the
19 regulations already explicitly make clear that OOPS
20 applies to pseudonymous profiles, the informational
21 session highlighted that many businesses are still
22 not meeting this requirement, and there are areas for
23 further guidance. In addition, several written
24 comments have also requested further guidance. So
25 staff recommends adding an example that highlights

1 the normative standard demonstrated in the Disney
2 matter, particularly with respect to tracking
3 technologies used for cross-context behavioral
4 advertising. When a business associates consumer
5 data across devices and identifiers for advertising
6 purposes, it should apply the opt-out with the
7 corresponding breadth. I think that's the most basic
8 example we can start off with. Providing an example
9 will offer additional clarity for businesses. It
10 would reinforce the existing normative standard
11 reflected in the Disney matter, and it would also
12 respond to commenters' requests for guidance.

13 Importantly, framing it as an example rather than a
14 new rule would underscore how this is already part of
15 existing law, and it would avoid constraining current
16 or future enforcement efforts.

17 To our third topic, as you know, current
18 regulations require businesses that process the
19 personal information of at least 10 million consumers
20 to annually disclose in their privacy policy metrics
21 regarding the CCPA requests that they receive,
22 respond to, etc. So these metrics include requests
23 to opt-out of sale and sharing. Staff recommend two
24 amendments to this provision. First, we recommend
25 requiring businesses to specify how many opt-out

1 requests were submitted through OOPS, including those
2 initiated via GPC. And second, we recommend
3 replacing the existing 10-million-consumer reporting
4 threshold with a standard that applies to any
5 business whose processing of personal information
6 poses a significant risk to consumer security or
7 privacy. As you may recall, that is the explicit
8 standard that would trigger a cybersecurity audit or
9 risk assessment.

10 The benefits of these changes are
11 three-fold. First, they would strengthen consumer
12 trust by providing a single and consistent location
13 in the privacy policy where consumers can confirm
14 large-scale compliance with OOPS-based opt-out
15 requests. Second, they would assist enforcement
16 efforts by making key CCPA metrics easily accessible
17 for corroboration by regulators and the public. And
18 third, they apply CCPA reporting obligations to all
19 businesses whose processing activities present
20 significant security and privacy risks, as reflected
21 by their inclusion in the mandatory cybersecurity
22 audit and risk assessment requirements, thereby
23 aligning reporting with the CCPA's risk-based
24 approach.

25 To the extent that the Board is concerned

1 with the cost to businesses for complying with these
2 two provisions, our preliminary estimates, drawing
3 upon the cybersecurity audit and risk assessment
4 analysis that we did previously, would indicate that
5 the burden is relatively modest. This is because
6 businesses are already required to keep records of
7 the CCPA requests that they receive and how they
8 respond to them for at least 24 months, and all
9 businesses are required to update their privacy
10 policies on a yearly basis. So, under a conservative
11 assumption that all businesses subject to CCPA would
12 have to now publish their metrics, the total
13 estimated cost is roughly around \$1.53 million. This
14 figure reflects half an hour of administrator or
15 developer time, at a blended rate per hour, to update
16 their website disclosures. While this estimate may
17 need to be refreshed to account for current wage
18 levels and updated business counts, it is likely
19 overstated, because many businesses are already
20 providing these disclosures on their website.

21 Finally, our last recommendation concerns
22 timing issues. The CCPA regulations make clear that
23 businesses must stop selling and sharing personal
24 information as soon as feasibly possible after
25 receiving a consumer's opt-out request, and no later

1 than 15 business days. In addition, if a business
2 continues to sell or share personal information
3 during the period before it fully processes the
4 request, it must notify all third parties that
5 received that information so those sales and shares
6 can be remedied. So, this framework applies equally
7 to online environments, where sales and sharing of
8 personal information often occur within milliseconds
9 of a page loading or cookie firing, as highlighted
10 during the informational session. However, many
11 businesses do not check for GPC before deploying
12 their tracking technologies that sell or share
13 personal information. This results in non-compliance
14 with both OOPS obligations and the timing
15 requirements already set forth in the regulations.
16 Several commenters, including privacy attorneys,
17 consent management platforms, and industry
18 participants, have raised similar concerns during the
19 public comment period.

20 So accordingly, staff recommend adding an
21 example that demonstrates proper compliance,
22 specifically detecting and honoring GPC before
23 deploying cookies or other tracking technologies that
24 sell or share personal information. Given the speed
25 at which online sales and shares are occurring,

1 detecting and honoring OOPS at the outset is both
2 feasible and essential. Otherwise, businesses risk
3 immediately selling or sharing personal information
4 and later facing the difficult and impractical task
5 of attempting to remedy those disclosures under the
6 regulation, section 7026(f)(2). So providing this
7 clarification through an example, rather than a new
8 regulatory amendment, ensures that the Agency does
9 not inadvertently suggest that the existing law is
10 unclear, or undermine current or future enforcement
11 actions. And to be clear, this example would reflect
12 existing requirements. The example simply offers
13 additional guidance to help businesses comply.

14 So together, these four recommendations
15 are intended to address issues raised by the public,
16 to provide clear guidance to businesses, and to
17 strengthen compliance with existing law and reinforce
18 the effectiveness of OOPS as a tool for consumers.
19 With that, I'm happy to hear your thoughts and any
20 questions you may have.

21 CHAIR URBAN: Thank you, Ms. Kim. Thank
22 you, Ms. Grenda. That was both -- that was very
23 clear and helpful. Thank you both.

24 Does staff recommend that the Board take
25 action today to direct staff to develop the materials

1 to be ready to commence a formal rulemaking in our
2 next meeting? Is that the process-based
3 recommendation here?

4 MS. KIM: I think the process would be
5 to, yes, direct us to get ready to engage with formal
6 rulemaking. Of course, once we have draft language
7 and text, that would come back to the Board for the
8 Board to review and finally approve.

9 CHAIR URBAN: Yes. But staff are ready
10 to go ahead and prepare the draft language, the
11 initial statement of reasons, and so forth for the
12 Board to consider.

13 MS. KIM: Yes.

14 CHAIR URBAN: Okay. Right. I just
15 wanted to be sure we all knew what we were thinking
16 about from a process perspective as we go into any
17 comments or questions from the Board.

18 Are there any?

19 Board Member Hamer?

20 MS. HAMER: Yeah. Thank you. It was a
21 very clear presentation. There we go. Thank you for
22 a very clear presentation. One of the items in the
23 summary was AI handling of GPC. So was there a
24 thought given to that, because that's going to be
25 kind of like a landslide at some point, and I think

1 it'd be good to get ahead of it?

2 MS. KIM: Yes. Thank you for that
3 question. We did think through and consider whether
4 or not that topic was right for consideration for
5 rulemaking or regulation, in particular. I think we
6 need some additional time to truly understand how
7 that AI or agentic AI works on a high level. I think
8 what we see in the marketplace right now is not -- is
9 more with regard to browsers having AI features that
10 go and search for information and then summarize and
11 provide to the consumer. So the consumer's actually
12 not going anywhere. They're staying within that
13 platform discussion. And in light of that, we still
14 need to do more factual understanding as to how our
15 law applies to that factual scenario and whether it's
16 applicable here.

17 But that said, it's certainly something
18 that we're carefully watching and engaging with and
19 thinking through. I would say at this time, we don't
20 think it's right for a regulation at this moment.

21 MR. LAIRD: And I'll just bolster that to
22 say. One thing we kind of kept coming back to is,
23 the beauty of CCPA is how agnostic it is to the
24 technology it's potentially regulating. And so in
25 many regards, I think we also thought through this,

1 and you come back to, well, the rules as written
2 apply sort of regardless. You know, a developer of
3 AI technology, you know, a business you engaged to
4 use AI technology still has -- is obliged by the same
5 opt-out requirements of sale and sharing as any other
6 business. And so in some regard, I think to Ms.
7 Kim's point, what we're waiting to observe is if
8 there is an alternative use that somehow brings into
9 question exactly how those rules apply. But
10 otherwise, we also think there's some simplicity here
11 that businesses should be able to translate on its
12 face. Simply put, they cannot sell or share your
13 personal information, whether it's through an AI tool
14 you are using on -- through them or otherwise, if
15 you're given that signal -- if you've given that
16 direction.

17 CHAIR URBAN: Thank you.

18 Please, do you have follow up, Ms. Hamer.

19 MS. HAMER: Perhaps even an example being
20 added might help clarify that it actually does apply,
21 because I doubt that developers think it does. I
22 think a lot of the language is specific around
23 browsers, and we have some issues around other types
24 of devices and smart devices. And AI is already
25 doing things, probably, that are contrary to what --

1 that they should be doing.

2 MR. LAIRD: Yeah. That's absolutely
3 helpful feedback. And I don't disagree that belt and
4 suspenders is also helpful always when it comes to
5 regulation. So I mean, I think it's certainly
6 something we could explore at the staff level
7 further, even if we feel like it's a restatement of
8 plain meaning of the law. I take the point
9 certainly, that that doesn't hurt and could help more
10 compliance.

11 CHAIR URBAN: Thank you.

12 Board Member Liebert?

13 MR. LIEBERT: Okay. Thank you. I'm
14 looking at our wonderful website privacy.CA.gov. And
15 I see some great helpful information on how Drop
16 works. And I'm wondering if we should consider doing
17 something similar in regards to OOPS and GPC that,
18 you know, educate -- we have some actually good
19 educating materials I've seen on the site for
20 businesses, but I don't know that we do -- and maybe
21 I'm just missing it -- in regards to consumers.

22 MS. KIM: I think perhaps Tom might be
23 the best person to respond to this.

24 MR. KEMP: Yeah. Sure. So we have put
25 forth about ten privacy tips, and that's one of the

1 top privacy tips --

2 MR. LIEBERT: Okay.

3 MR. KEMP: -- we have. And then I did a
4 couple blog posts on that as well. And -- but
5 really, the big focus will be in January when the
6 browser vendors support it. And so we're going to go
7 really hard. And I think Ms. White will talk more
8 about this --

9 MR. LIEBERT: Okay.

10 MR. KEMP: -- tomorrow. So I'm not going
11 to say anything more because that's a topic. But
12 you'll get a good feel for what's happening as it
13 relates to further promotion of this directly to
14 consumers.

15 And the other thing I'll add is, is that
16 we've built up an incredible mailing list for
17 newsletter subscribers. And so this gives us a great
18 opportunity come January to promote the fact that now
19 with all these major browsers, here are the specific
20 directions that you can use to turn it on.

21 So in summary, content does exist. I
22 think we also created a video for consumers as well.
23 But the big push will happen come January.

24 MR. LIEBERT: And that content, then, it
25 sounds like, will be put on the website, as well.

1 MR. KEMP: Oh, absolutely. There is
2 content now under the privacy tips. Also, if you
3 look at the senior scammers, we are teaching senior
4 citizens how to turn that on as well when we do those
5 events. And so it's been integrated. It's one of
6 our top -- the easiest one is Drop. The second
7 suggestion that we have is to turn on OOPS. And so
8 the thought process is, if you spend 5, 6, 7 minutes
9 on Drop, you spend 30 seconds. If it's a browser
10 that supports it, or you download a third-party
11 extension, maybe you spend another minute or two.
12 And that's kind of the 20/80 rule that you get a lot
13 of great coverage with third parties with Drop, and
14 then the opt-out of sale and sharing with first party
15 interactions as well. But it really makes sense come
16 January, when we can explicitly tell people on
17 Chrome, go to this, this, this. Same thing with
18 Safari, same thing with Edge. And so we will be very
19 prescriptive, and that will be a big focus of our
20 campaigns come January.

21 CHAIR URBAN: Thank you. Additional
22 comments or questions?

23 All right. So maybe this will prompt
24 some or maybe not. So taking into account the
25 substantive recommendations from staff and what I

1 understand the process to be, I will request a motion
2 to direct staff to prepare all documents and
3 materials necessary to open formal rulemaking for the
4 regulatory changes staff recommended today and in
5 alignment with today's discussion, and to bring draft
6 text implementing those recommendations before the
7 Board, again, before commencing the 45-day public
8 comment period.

9 Mr. Laird, did I cover the necessary?

10 MR. LAIRD: Yes. Perfect.

11 CHAIR URBAN: Okay. Great. So that will
12 be the motion I will request. And at this point, I
13 would like to ask if there's any public comments on
14 this item.

15 MS. CARWILE: This is for Agenda Item 3,
16 Preliminary Rulemaking Update and Recommendations on
17 Opt-Out Preference Signals. If you'd like to make a
18 comment at this time, please raise your hand using
19 the raised hand feature or by pressing star-nine if
20 you are joining us by phone. This is for Agenda Item
21 3.

22 Madam Chair, I'm not seeing any hand
23 raised at this time.

24 CHAIR URBAN: Okay. Thank you, Ms.
25 Carwile.

1 And with that, I will request from the
2 Board the motion as stated. Is anyone ready to make
3 the motion?

4 Mr. Liebert makes the motion. Is there a
5 second?

6 MS. OZER: Second.

7 CHAIR URBAN: Thank you. I have a motion
8 on the table and a second motion from Mr. Liebert,
9 second from Ms. Ozer.

10 Ms. Carwile, would you please conduct the
11 roll call vote?

12 MS. CARWILE: Yes, this is a roll call
13 for the motion as stated by the Chair.

14 Board Member Hamer?

15 MS. HAMER: Aye.

16 MS. CARWILE: Board Member Liebert?

17 MR. LIEBERT: Aye.

18 MS. CARWILE: Board Member Mactaggart?

19 Board Member Ozer?

20 MS. OZER: Aye.

21 MS. CARWILE: Chair Urban.

22 CHAIR URBAN: Aye.

23 MS. CARWILE: Madam Chair, you have four
24 yeses and one not voting.

25 CHAIR URBAN: Thank you very much, Ms.

1 Carwile. And thanks everyone on the Board and of
2 course, to our wonderful staff for that very
3 thoughtful and efficient presentation. The motion
4 has been approved by a vote of four to zero.

5 We will now move on to Agenda Item 4,
6 which is Discussion and Possible Action to Amend
7 Regulations Section 7500 Conflict of Interest Code,
8 Including Possible Adoption of Proposed Text. You
9 have materials before you with the proposed text.
10 And as a reminder to the Board, we discussed this in
11 our last meeting. This is bringing our legally
12 required conflict of interest code up to code,
13 because we now have about 70/75 people. And when we
14 first adopted it in our very first board meeting, we
15 had none. And anticipate an executive director and
16 something. So to cast you back into what we have
17 already discussed. That's what's up today.

18 And I will ask Mr. Laird, who's going to
19 present this, to go ahead.

20 MR. LAIRD: Thank you, Chair Urban. And
21 I agree, this should be a relatively quick
22 discussion. This, if this looks familiar, it's
23 because it's the exact same text you saw at our last
24 meeting, but that was to get your approval to begin
25 the comment period. We have since held the comment

1 period. We received no comments from the public
2 during that time. We did make the edit that Ms. Ozer
3 pointed out -- there, the extraneous 'that' has been
4 removed. And at this point we are asking for your
5 adoption of these amendments. And the process, just
6 for your awareness, would be: If you adopt, then
7 it'll go back to the Fair Political Practices
8 Commission for their final approval, and then be
9 filed and take effect within 90 days of its filing
10 with the Office of Administrative Law.

11 CHAIR URBAN: Thank you very much,
12 Mr. Laird. Any Board questions or comments on this?

13 All right. And then I will request the
14 motion to adopt the conflict of interest code
15 amendments as proposed and to direct staff to take
16 all steps necessary to complete the rule making
17 process, including filing the final rulemaking
18 package with the Office of Administrative Law, the
19 amendment of any documents within the rulemaking
20 package other than the text of the rules as necessary
21 to ensure clarity, accuracy, and compliance with the
22 Administrative Procedures Act, and authorizing the
23 executive director to make any non-substantive
24 changes to the proposed regulations, and to further
25 authorize staff to withdraw the rulemaking and

1 file -- in whole or in part -- in consideration by
2 the Office Of Administrative Law at any time if in
3 their opinion, the legal risks associated with
4 disapproval of these regulations warrant further
5 consideration by the Board. That will be the motion
6 that I will request in case you were wondering, which
7 I'm sure you were not. I had that one written down.

8 And I will ask if there's any public
9 comment.

10 MS. CARWILE: This is for Agenda Item 4,
11 Discussion and Possible Action to Amend Regulation
12 Section 7500 Conflict of Interest Code, Including
13 Possible Adoption of Proposed Text. If you'd like to
14 make a comment at this time, please raise your hand
15 using the raised hand feature or by pressing
16 star-nine if you're joining us by phone. This is for
17 Agenda Item 4.

18 Madam Chair, I'm not seeing any hands
19 raised at this time.

20 CHAIR URBAN: Thank you, Ms. Carwile.
21 In that case, may I have the motion as
22 stated? Thank you. I have a motion from Ms. Hamer.
23 May I have a second?

24 MR. LIEBERT: Second.

25 CHAIR URBAN: Thank you. The motion as

1 stated is made by Miss Hamer, seconded by Mr.
2 Liebert, Ms. Carwile, would you please conduct the
3 roll call vote?

4 MS. CARWILE: Yes, this is a roll call
5 for the motion as stated by the Chair.

6 Board Member Hamer?

7 MS. HAMER: Aye.

8 MS. CARWILE: Board Member Liebert?

9 MR. LIEBERT: Aye.

10 MS. CARWILE: Board Member Mactaggart?

11 Board Member Ozer?

12 MS. OZER: Aye.

13 MS. CARWILE: Chair Urban.

14 CHAIR URBAN: Aye.

15 MS. CARWILE: Madam Chair, you have four
16 yeses and one not voting.

17 CHAIR URBAN: Thank you very much. The
18 motion has been approved by a vote of four to zero.
19 I thank the staff for all your work to keep us up to
20 date and everyone for making their disclosures, so
21 the public is able to judge what we are doing by
22 those disclosures. Very much appreciated. And thank
23 you for the efficient process today. Thanks again to
24 our speakers who, again, were incredibly informative
25 and helpful. And to the team who put together the

1 informational session for us. We have found these
2 very valuable. And as Mr. Liebert suggested earlier,
3 I think we're very much looking forward to the others
4 as well. Before we end for today and start back
5 tomorrow, I believe our executive director, Mr. Kemp,
6 has something to say.

7 Okay. Mr. Laird?

8 MR. LAIRD: I think we were just going to
9 note, knowing that it's a full agenda tomorrow, I
10 didn't know if the Board wanted to consider taking
11 any of the items for tomorrow, specifically,
12 potentially future agenda items. We could still wait
13 till tomorrow as well, but.

14 CHAIR URBAN: Okay. Yes. I was trying
15 to be kind, but it does mean being mean tomorrow. So
16 I will ask the Board what their preference is.

17 Would you like to discuss future agenda
18 items now, or would you like to wait until tomorrow?

19 MS. HAMER: I would prefer to wait until
20 tomorrow for one.

21 CHAIR URBAN: Okay. All right. In that
22 case, let's go ahead and be in recess until 9:00
23 tomorrow morning, August 7th, when we will continue
24 with the agenda as posted on our website and here in
25 San Francisco. Thank you all very much. The Board

1 is now in recess.

2 (End of audio recording.)

3 -000-
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25