

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

CALIFORNIA PRIVACY PROTECTION AGENCY

TRANSCRIPTION OF RECORDED PUBLIC MEETING

MARCH 29, 2022

SACRAMENTO, CALIFORNIA

Present: LYDIA DE LA TORRE, Board Member
VINHCENT LE, Board Member
ANGELA SIERRA, Board Member
J. CHRISTOPHER THOMPSON, Board Member
JENNIFER M. URBAN, Chair
JUSTIN GOURLEY, Moderator
ASHKAN SOLTANI, Presenter
LISA KIM, Presenter
JENNIFER KING, PH.D., Presenter
LIOR J. STRAHILEVITZ, Presenter
LORRIE FAITH CRANOR, D.SC., Presenter
STACEY SCHESSER, Presenter

Transcribed by: Brittany D. Payne,
eScribers, LLC
Phoenix, Arizona

1 **TRANSCRIBED RECORDED PUBLIC MEETING**

2 **March 29, 2022**

3 **MS. URBAN:** Good morning. Welcome to the California
4 Privacy Protection Agency's March 2022 pre-rulemaking
5 informational sessions. My name is Jennifer Urban. I'm
6 the chairperson for the Board for the agency. Other
7 members of the Board are here with me this morning.

8 Good morning, everyone. It's really wonderful to
9 see you all, and I'm looking forward to today and
10 tomorrow. I now call the meeting to order and would like
11 to ask our moderator, Mr. Justin Gourley, to please
12 conduct the roll call.

13 **MR. GOURLEY:** Okay. Thank you, Chairperson Urban.
14 I will start the roll call now. Ms. De la Torre.

15 **MS. DE LA TORRE:** Present.

16 **MR. GOURLEY:** Mr. Le.

17 **MR. LE:** Present.

18 **MR. GOURLEY:** Ms. Sierra.

19 **MS. SIERRA:** Present.

20 **MR. GOURLEY:** Mr. Thompson.

21 **MR. THOMPSON:** Present.

22 **MR. GOURLEY:** Chairperson Urban.

23 **MS. URBAN:** Present.

24 **MR. GOURLEY:** Chairperson Urban, five board members
25 are present.

1 **MS. URBAN:** Thank you, Mr. Gourley.

2 The Board has established a quorum. Thank you very
3 much, board members.

4 For everybody's edification, we are having
5 informational sessions today, which I'll describe a
6 little bit more in a minute. So for the most part, board
7 members will have our cameras off as we will be listening
8 to the presentations along with you.

9 So before I get started with the substance of the
10 day, I, as usual, have some logistical announcements.
11 First, I'd like to ask that everyone please check your
12 microphone is muted with when you're not speaking.
13 Please also note that this meeting is being recorded.

14 Meetings and events involving a majority of the
15 Board, include informational and instructional sessions
16 like these, will be run according to the Bagley-Keene
17 Open Meeting Act as required by law. I'll first
18 introduce the format for these pre-rulemaking
19 informational sessions and then explain the mechanics of
20 public comment today. First, let me sketch the format of
21 these informational sessions so everyone has a sense of
22 how things will proceed.

23 Each day includes a set of expert presentations that
24 will provide background information on topics that are
25 potentially relevant to our upcoming rulemaking. I will

1 open the session each day, and then we'll go into one
2 item each day comprising a series of presentations on
3 that day's topic.

4 Now let me talk about to engage in public comment.
5 I will call for public comment after each item, so that
6 is after our introductory item each day, and then after
7 the presentations each day. Each speaker will be limited
8 to three minutes. If you wish to speak on an item,
9 please use the "raise your hand" function, which can be
10 found in the reaction feature at the bottom of your Zoom
11 screen.

12 Our moderator will request that you unmute yourself
13 for comment. When your comment is completed, the
14 moderator will mute you. It is helpful if you identify
15 yourself, but this is entirely voluntary, and you can
16 input a pseudonym when you log into the videoconference.

17 I would like to remind everyone of the rules of the
18 road under Bagley-Keene. Bagley-Keene requires that
19 comments be tied to the agenda items. Accordingly,
20 please plan to comment on today's presentations at the
21 end of today's session and tomorrow's presentations at
22 the end of tomorrow's session. I'd like to remind
23 everyone to stay on topic, and please keep your comments
24 to three minutes or less.

25 Now, a little bit more about the schedule. Today we

1 plan to take a break for lunch after the first two
2 informational presentations, depending on where we are on
3 the schedule, and we'll take some shorter breaks if
4 they're needed. Tomorrow we'll do the same.

5 As I mentioned, this is being recorded. We also
6 should have a transcript once that can come together. So
7 there will be -- you know, you'll be able to see the
8 information later if you need to come and go outside of
9 breaks.

10 My thanks to all the expert speakers who are taking
11 time to present to us today and tomorrow and to all the
12 people working to make this meeting possible. I would
13 like to especially thank the team from the Office of
14 Attorney General supporting us today: Mr. Malaud Valdu
15 (ph.), who is acting as our counsel; Mr. Justin Gourley,
16 who is acting as the moderator; Ms. Trina Hurtado (ph.),
17 who is the conference services expert who's organized the
18 meeting infrastructure; and Ms. Stacy Hindson (ph.) for
19 organizing administrative staffing and resources.

20 I'd also like to thank the team at the Department of
21 Consumer Affairs for managing our communications link and
22 website technology generally. I would also like to thank
23 the staff at the Business, Consumer Services and Housing
24 Agency, the Department of Consumer Affairs, the
25 Department of General Services, the Office of the

1 Attorney General, and other agencies who continue to help
2 behind the scenes.

3 Before we move to today's presentations, I'd also
4 like to take the opportunity to provide an update on our
5 program of pre-rulemaking informational hearings and to
6 invite your participation. We have announced two sets
7 pre-rulemaking events, first, these informational
8 sessions that we're holding today and tomorrow, and
9 second, stakeholder sessions.

10 As I mentioned, the pre-rulemaking informational
11 sessions today and tomorrow will provide background
12 information on various topics potentially relevant to our
13 rulemaking. The speakers for these informational
14 sessions are academics who study relevant topics and
15 officials from the California Office of the Attorney
16 General, California Privacy Protection Agency, and the
17 European Data Protection Board. We hope that these will
18 provide helpful information. It is important to note
19 that our guest presenters' view should not be taken as
20 the views of the agency or the Board. They are the views
21 of the presenters only.

22 Our second set of pre-rulemaking events will be the
23 pre-rulemaking stakeholder sessions, which we plan to
24 follow a month or so from now. The stakeholder sessions
25 are designed to gather stakeholder input, which is

1 complimentary to the written stakeholder input we
2 received in response to our preliminary invitation for
3 comment. Like the written input, this information will
4 be very helpful. There are many knowledgeable
5 stakeholders who can offer input based on their specific
6 experience and expertise.

7 I also want to be clear about what I mean by
8 expertise here. Today and tomorrow's speakers, of
9 course, are people who've studied the topics they're
10 talking about in a formal way. Expertise comes in many
11 forms. Stakeholders of all types have experiences and
12 expertise that will be extremely helpful, for example, an
13 individual business' experience with the law, a
14 consumer's experience with their work to try to
15 understand and exercise their rights, a nonprofit that
16 works with consumers, or an association that will work
17 with businesses. All of those perspectives and more will
18 be very helpful in understand the backdrop of our
19 potential regulations.

20 So I encourage everyone who's interested in
21 participating to sign up for the stakeholder sessions.
22 You can find more information on our website,
23 cpa.ca.gov, on the regulations page. You'll find there
24 information about logistics and a link to a sign-up form.
25 Please note that the date for the stakeholder sessions is

1 not yet set because staff are working on venue options
2 that will allow us to have an in-person portion. But
3 please do feel free to sign up now because the agency
4 will contact you with options for participation, and
5 you're always free to decline if the final dates are
6 inconvenient for you.

7 Also, if we get to the stakeholder sessions and you
8 haven't remembered to sign up, there will be
9 opportunities for general public comment as well. So
10 please check it out, and please consider participating.
11 We would really value your input. And if you have
12 questions, please feel free to write to info@coppa.ca.gov.

13 I'd also like to extend my usual invitation to sign
14 up for any of our email lists if you would like to
15 receive announcements. You can find those on the CPPA
16 website under "Contact us."

17 All right. We will next move to the informational
18 presentations for the day. Before we do, is there any
19 public comment from those in the audience?

20 **MR. GOURLEY:** As a reminder, if you would like to
21 comment, please press the "Raise hand" icon on your
22 screen. For those of you using dial-in function, you may
23 press star nine to indicate that you would like to
24 comment. Once I've called on you, you the star six
25 command to unmute yourself. You'll then be called on and

1 have up to three minute to make your comment.

2 **MS. URBAN:** Thank you, Mr. Gourley.

3 **MR. GOURLEY:** There's one comment. Sorry.

4 **MS. URBAN:** Okay.

5 **MR. GOURLEY:** Sharon (ph.), you are now unmuted.

6 **SHARON:** Thank you. Could you do me a favor and

7 clearly define what a stakeholder means? I'm unmuted.

8 **MS. URBAN:** I would suggest that you go to the

9 website and read more information about the sessions, but

10 anyone who has an interest in the topics under the

11 agency's jurisdiction.

12 **SHARON:** Okay. Great. So us persons participating

13 in this meeting this morning or listening into this

14 meeting are considered stakeholders?

15 **MS. URBAN:** Sure.

16 **SHARON:** Thank you.

17 **MR. GOURLEY:** Thank you.

18 **MS. URBAN:** Mr. Gourley, is there anyone else?

19 **MR. GOURLEY:** There is no one else.

20 **MS. URBAN:** Okay. Let's just wait for a little

21 while and see if people are formulating thoughts, and

22 then if not, we will go to the next item.

23 **MR. GOURLEY:** There is nobody else at this time.

24 **MS. URBAN:** Thank you very much, Mr. Gourley.

25 And thank you for the public comment we received.

1 We will now move to the informational presentations
2 for the day. The topic of the presentations together is
3 overview of personal information and the California
4 Consumer Private Act. You can follow along on the
5 agenda, and again, please note we will take some breaks.

6 I'll introduce each speaker with a short biography,
7 and then they will present to us. I understand that
8 speaker bios and the slide presentations, if there are
9 any that speakers use today, will be available on the
10 CPPA website as soon as they can be processed, along with
11 the recording and the transcript. So there should be
12 plenty of opportunities to review the information if
13 you'd like.

14 Our first presenter is Ashkan Soltani. Mr. Soltani
15 is the executive director here at the California Privacy
16 Protection Agency. He is providing a presentation today
17 on data flows; that is, how consumer information is
18 collected and how it flows to the data ecosystem. Excuse
19 me.

20 Mr. Soltani, prior to coming to the agency, had been
21 a researcher and technologist specializing in private,
22 security, and technology policy. He has focused his work
23 on researching, understanding, and describing privacy
24 issues online and explaining technology for those who are
25 not experts, making him well-placed to describe data

1 flows for us today.

2 Mr. Soltani has previously served as a senior
3 advisor to the US chief technology officer in the White
4 House Office of Science and Technology Policy and as the
5 chief technologist for the Federal Trade Commission,
6 advising the commission on its technology-related policy
7 as well as helping to create its Office of Technology
8 Research and Investigation. He has also contributed to
9 multiple prize-winning investigative journalism teams
10 looking to understand various collections and uses of
11 data. He holds a bachelor's degree in cognitive
12 science from the University of California-San Diego and a
13 master's degree from The School of Information at the
14 University of California-Berkeley.

15 Welcome, Mr. Soltani, and I will turn things over to
16 you.

17 **MR. SOLTANI:** Thank you, Chairperson Urban. Can you
18 all see my presentation?

19 **MR. GOURLEY:** Yes, we can.

20 **MR. SOLTANI:** Perfect. Good morning, everyone. As
21 the chairperson mentioned, we'll get started today with a
22 brief overview of the types of data flows consumers might
23 encounter as they navigate throughout their daily lives.
24 Note, this presentation is fairly high level and is
25 not intended to be exhaustive. It sketches out some of

1 the common data flows to help ground further discussion.

2 Data about us are collected and shared constantly.
3 For example, when we go to the store, we might provide or
4 name and address to a business in order to buy something
5 or register for a warranty. That data might also be
6 shared with a service provider, for example, with a
7 logistics company to fulfill the item or to a third party
8 such as a data broker to generate a secondary revenue
9 source for the business.

10 Similarly, when we browse the web, we also share
11 data with businesses. We may fill out a form, looking up
12 a dictionary word, or provide our email address to a
13 website in order to subscribe to the word-of-the-day
14 mailing list. This is information we intentionally share
15 with one or more parties.

16 Our information is also shared with businesses as a
17 result of how the technology is designed. For example,
18 as we surf the web, businesses automatically receive
19 information about us, including our IP address,
20 information about the type of browser and computer we're
21 using, cookies and other identifiers, which I'll get into
22 later in this presentation, our location, and if a user
23 has enabled a global privacy control, their opt-out
24 preference.

25 Like the retail example, these data are typically

1 shared not only with the business the consumer intends to
2 interact with, but with service providers and third
3 parties. For example, in this image, some of the ads,
4 images, and underlying software facilitate the
5 transmission of consumers' data with a number of third
6 parties that the consumer is not directly interacting
7 with. These can be advertisers, analytics companies,
8 security providers, and data brokers. These entities can
9 be service providers to the business or, more commonly,
10 third parties.

11 Some data flows through elements that are not
12 visible to the user. For example, many websites use
13 third-party code, often known as pixels, to enable
14 service providers and third parties to identify the user
15 and monitor their browsing activities. How individuals
16 are identified on the internet can vary. We're familiar
17 with the idea that our identities are tied to our name,
18 address, birth date, but there are other, often more
19 robust ways to identify individuals. Social Security
20 numbers are one well-known example, but other such as
21 email addresses, phones, device IDs all serve the same
22 purpose.

23 In the examples before, I mentioned cookies, which
24 are often unique strings of numbers and letters assigned
25 to you by websites you encounter. Your browsers then

1 store and transmit these identifiers every time you
2 encounter the website, which enables those sites and
3 services to uniquely identify you. Your phone also has a
4 number of other unique IDs, especially -- specifically
5 for profiling and targeting of advertisements, including
6 a handful of immutable unique identifiers that uniquely
7 identify your device and never change.

8 Mobile devices also contain a variety of antennas,
9 such as GPS and Bluetooth, and sensors, for example,
10 accelerometers and cameras, that regularly collect and
11 make information available about us, and since we carry
12 these devices with us every day and interact with them
13 throughout the day, the volume of that data linked back
14 to us can be significant.

15 Information about our location, what apps we're
16 using, who we call, and our list of friends and contacts
17 all are often stored and shared. For example, when you
18 use a locational wear app to look up a local restaurant,
19 your phone will typically reviewal your location, your
20 identity, and possibly your food interests to one or more
21 parties.

22 And just as with the web, as users interact with
23 their devices and mobile applications, and sometimes when
24 they don't, as in the case of background applications and
25 operating systems, that software can subsequently share

1 and sell data with a number of parties beyond the
2 original person or app the user shared with.

3 Finally, because of their size and the way mobile
4 apps are designed and the fact that we often use them on
5 the run, smartphones often tend to be more limited in the
6 way they can display notices and make users aware of data
7 sharing that might occur.

8 Here is an example of the various parties that might
9 receive a user's location information. These include the
10 mobile device manufacturer, the enhanced location
11 provider, if there is one, the wireless service provider,
12 the third-party location aggregators, and finally mobile
13 apps, like the restaurant finder I mentioned. All of
14 these parties may then further sell or share that
15 information.

16 As we move into a world of internet-enabled devices,
17 additional data flows come into being. Health monitors,
18 smart thermostats, internet-connected TVs, and smart
19 sneakers start -- excuse me, smart speakers enable a host
20 of data uses which enable us to automate our daily lives,
21 monitor our health, and optimize our energy usage. These
22 internet of things, or IOT devices, thereby generate a
23 great deal of information about us, such as whether we're
24 home, when we're asleep, what shows we watch, and how
25 active we are at night.

1 As with other technologies, often these data flow
2 beyond the confines of our home to businesses and third
3 parties and other entities consumers aren't directing --
4 aren't interacting with directly. For some IOT devices,
5 it may be difficult for consumers to know what these
6 underlying practices are. Some of these devices, for
7 example, don't have screens or may have become bundled as
8 part of a purchase.

9 Modern vehicles also have some of the same
10 properties as smartphones and IOT devices. In fact, cars
11 with remote access capabilities, like we see in some EVs
12 and newer luxury vehicles, operate much like smartphones.
13 They're often equipped with GPS, accelerometers, and
14 cameras that monitor the occupant's location and
15 activities. They can, for example, provide driving
16 directions, alert the driver when they're drowsy, or
17 monitor how aggressively someone accelerates in order to
18 score their driving habits. Depending on the features
19 the owner consents to or the manufacturer or dealerships
20 select, the car may share this information with a number
21 of third parties.

22 As I mentioned, often our modern devices share
23 information with third parties. These third parties then
24 use information they collect from one or more businesses
25 to inform what a consumer might do on other businesses.

1 The collection and correlation of these activities across
2 businesses create a profile about the user, and this
3 profile is used to inform the ads of products it shows a
4 user, how many times the ad was shown, whether a given ad
5 was successful, for example, if the user purchased
6 something as a result of seeing an ad, or make inferences
7 about the user outside of the advertising space
8 altogether, for example, related to media preferences,
9 politics, and other inferred behaviors.

10 Profiles aren't always used for advertising.
11 Websites can also use -- sorry. Websites can also target
12 ads based on the context of the website, not the profile
13 of the user. For example, you can show car ads on an
14 automobile enthusiast website without the reliance and
15 sale and transfer of personal information.

16 Contextual advertising, as this is described, is a
17 long-standing method of delivering ads. There are also
18 newer methods that allow targeted advertising and even
19 conversion tracking, which I described as measuring
20 whether an ad was successful without relying on the sale
21 and sharing of a user's data across sites. Presently the
22 status quo, however, is to create a profile of the user
23 as they traverse the internet for this and many other
24 purposes.

25 The previous slide showed the perspective of one

1 party collecting data across a variety of websites and
2 devices. However, websites, mobile apps, and publishers
3 typically rely on networks of advertisers, typically
4 third parties, who bid for and serve ads using an
5 exchange. This looks similar to a stock exchange. When
6 a user visits a website or uses a mobile app that relied
7 on an ad exchange, their information is often made
8 available not only for -- to the network exchange, but to
9 hundreds of advertisers and data brokers the user does
10 not direct -- have a direct relationship with.

11 The user's information is typically shared and
12 stored by all of the potential bidders, regardless of
13 whether or not the advertiser provides the winning bid.
14 Typically there are dozens, if not hundreds, of
15 advertisers that participate in each auction and millions
16 of auctions every minute, which results in a great volume
17 of consumers' data being automatically transferred
18 downstream.

19 Much of the information that I just described, as
20 well as additional data that I haven't described,
21 eventually flow to data brokers. Data brokers are
22 companies that use data to profile consumers and resell
23 that information for various purposes, some of which
24 we'll hear about later today and tomorrow.

25 Some of these uses might be to identify potential

1 customers for new products, candidates for employment, or
2 who to reach out to for a nonprofit fundraiser. While
3 some of this information is collected directly from the
4 consumer, then sold and shared, other times the
5 information is purchased from other third parties, which
6 then further sellers share that user's data creating a
7 cycle of data flows that the subject has limited
8 visibility into. I trust the forthcoming presentation
9 will help eliminate some of those uses and consumer
10 remedies.

11 So in this presentation, I have covered some of the
12 typical ways consumers' data flow through the information
13 ecosystem, including the traditional retail space, on the
14 web, and through smartphones and other connected devices.
15 This was a basic overview, not an exhaustive review. For
16 example, brick-and-mortar retail locations that track
17 individuals as they move about their stores were not
18 mentioned. The purpose was just to provide basic
19 introduction to the data flows and ground further con --
20 excuse me, ground further discussions. Hopefully, it was
21 helpful. Thank you.

22 **MS. URBAN:** Thank you very much, Mr. Soltani, for
23 that helpful presentation.

24 Our next speaker is Ms. Lisa Kim, who will be
25 presenting on how the California Consumer Privacy Act

1 interacts with personal information data flows. After
2 Ms. Kim, we will take a lunch break. So we'll have one
3 more presentation before we do take a break.

4 Ms. Kim is a deputy attorney general in the privacy
5 unit of the Consumer Protection Section at the California
6 Department of Justice. Ms. Kim enforces state and
7 federal privacy laws, promulgates privacy regulations,
8 educates Californians on their rights and strat -- on
9 their rights and strategies for protecting their privacy,
10 encourages businesses to follow privacy respectful best
11 practices, and advises the Attorney General on privacy
12 matters.

13 As contemplated in the California Privacy Rights Act
14 of 2020, which created the CPPA, Ms. Kim is assisting the
15 CPPA in its work. Before joining the office, Ms. Kim
16 worked at an international law firm as a litigator with
17 experience in various areas of law, including
18 class-action defense, legal malpractice, products
19 liability, financial services, and privacy. Ms. Kim
20 earned her BA magna cum laude from the University of
21 California-Los Angeles and her JD from the University of
22 California-Berkeley School of Law. We're very pleased
23 that she is here with us today.

24 And Ms. Kim, the floor is yours. Thank you.

25 **MS. KIM:** Thank you very much. Let me go ahead and

1 share my screen. Okay. So I wanted to thank you first.
2 First of all, thank you for having me. I'm glad to be
3 able to give this presentation. This presentation is
4 called "How the CCPA Interacts with Personal Information
5 Data Flows." The goal for this presentation is to
6 basically give a general overview of the CCPA and the
7 CPRA amendments to the CPPA. It won't cover all aspects
8 of the CCPA, but primarily the rights that are given to
9 consumers and how those rights relate to the data flows
10 that were previously presented by Mr. Soltani.

11 As an initial matter, though, I always start with
12 this disclaimer, which is I work for the California AG's
13 office, but this presentation reflects my own views. It
14 does not necessarily reflect the views of the State of
15 California or the Attorney General.

16 So before we get started with regards to the
17 specific rights that consumers have under the CCPA, I
18 wanted to start off with some formative definitions
19 because they do frame our analysis and understanding of
20 how the CCPA is a CPRA, and I'll use those relatively
21 interchangeably, affect data flows.

22 So first off, let's talk about the definition of
23 business. So the definition of business under the CCPA
24 basically means a for-profit entity that does business in
25 California, that collects and processes consumer personal

1 information, and then also fits one of the following
2 criteria. Either it has an annual gross revenue in
3 excess of \$25 million or it deals with personal
4 information of 100,000 or more consumers or households.
5 Now, that is an increase, because the CCPA previously had
6 50,000 consumers or households, and the CPRA amendment
7 bumped it up to 100,000. And then finally or derives 50
8 percent or more of its annual revenue from selling or
9 sharing consumers' personal information, and this is
10 mainly targeted toward businesses that work with that --
11 that business seeks to sell or share consumers' personal
12 information, such as data brokers.

13 Now, the next definition I wanted to speak about is
14 personal information. Personal information is defined in
15 the statute, but it's defined very broadly. It means
16 anything basically reasonably capable of being associated
17 to a particular consumer or household and includes things
18 like identifiers, product and services used, biometric
19 information, geolocation information, even things like
20 olfactory information and inferences about a consumer.
21 There's also a newly specific subset of personal
22 information that is introduced by the CPRA, and that is
23 sensitive personal information, and that's separately
24 defined, and I'll go into that a bit more in detail later
25 in this presentation.

1 So with regard to the definition of personal
2 information as it pertains to the presentation that Mr.
3 Soltani gave, many of those identifiers and things that
4 he mentioned, such as cookies, can be considered personal
5 information. Now, there's one thing that is not included
6 in personal -- in the definition of personal information,
7 and that is public information, deidentified information,
8 and aggregate consumer information, and all three of
9 those terms are also separately defined in the CCPA.

10 Now to talk about the general key aspects of the
11 CCPA. The CCPA that is now in effect basically has the
12 following rights that are given to consumers: the right
13 to delete, the right to know, the right to equal service
14 or nondiscrimination, and the right to opt out of the
15 sale of personal information, and I'll go into this in
16 greater detail later on.

17 The CPRA amendments to the CCPA that are effective
18 January 1st, 2023, also add additional rights. Those
19 rights include expanded rights to opt out of the sharing
20 of personal information, the right to correct inaccurate
21 information, the right to limit the use and disclosure of
22 sensitive personal information, and also this idea of
23 data minimization and purpose limitations.

24 Now, before we get into this, I just wanted to point
25 out, in addition to the rights, there are certain

1 required disclosures that are provided by the CCPA.
2 These are obligations that a business has in giving
3 disclosures to consumers. There is an obligation to
4 provide a privacy policy, and this basically is a one-
5 stop shop where a consumer can find information about all
6 of the business's data practices as well as a description
7 of their CCPA rights and how to exercise them, and in
8 some instances, there are also requirements that a
9 business who holds or collects personal information of
10 more than 10 million consumers has to report the metrics
11 about the CCPA and the requests that have been made of
12 them.

13 There is also a notice of collection. A business
14 must inform a consumer at or before the collection of
15 personal information, the categories of personal
16 information it seeks to collect, as well as the purposes
17 for which they will be used, and there is an obligation
18 that if you do not properly disclose these purposes, that
19 you cannot use or collect those for any additional
20 purposes not disclosed.

21 There is also a required disclosure of certain
22 opt-out link. Under the CCPA, there's a "Do not sell my
23 personal information" link that needs to be posted on the
24 business' website if the business sells personal
25 information. And then the CPRA amendment added a "Do not

1 sell or share my personal information" as well as
2 separately the "Limit the use of my personal information"
3 link, and I'll go into that in greater detail later.
4 They also provide a general alternative offset link where
5 a consumer make both of those -- exercise both of those
6 rights at the same time.

7 And finally, just to note, there is a notice of
8 financial incentive that if a business is providing a
9 consumer with an incentive or a price-of-service
10 difference that is tied to the collection, sale or
11 sharing or retention of personal information, they must
12 provide a notice explaining the material terms.

13 Now, to talk about the first right with regard to
14 the delete with the CCPA, this -- you know, I wanted to
15 explain that this is generally a limited right because it
16 only pertains to personal information collected from the
17 consumer, and there are also some statutory exceptions
18 that apply. So for example, if the information selected
19 from the consumer is necessary to provide the good or
20 service, then the right -- the request to delete by the
21 consumer may be denied. Other things are security and
22 fraud prevention, issues where a business may have to
23 retain the personal information for a certain amount of
24 time given legal obligation, that sort of thing.

25 To overlay this right to delete with regard to the

1 data flows that Mr. Soltani previously discussed, this
2 right to delete applies to information from the
3 first-party business or the business in which the
4 consumer is expecting to interact with. So for example,
5 this right to delete would apply to, say, a retailer that
6 a consumer goes into their store and says -- you know, is
7 purchasing goods from. And if that retailer collects
8 personal information from the consumer, then the consumer
9 has the right to delete -- request to delete that
10 information.

11 It also applies to service providers. So for
12 example, if a consumer interacts with a business and that
13 business shares the information with a service provider,
14 that service provider would also have to delete that
15 information, but the request must go through the
16 first-party business, so the initial business that the
17 consumers interacted with. So it would apply to the
18 service provider, but through the first-party business.

19 From our experience in the DOJ just receiving
20 consumer complaints and that sort of thing, there are
21 some barriers that consumers do commonly face when
22 exercising the right or some misconceptions or confusions
23 that consumers may face. That includes misunderstanding
24 if not realizing that all these actuary (ph.) exceptions
25 do apply and may apply. There's also certain exceptions

1 that are provided for in the law itself that applies to
2 an entire title. They're set forth in Civil Code Section
3 1798.145 and includes things like certain information
4 that is already governed under a different legal law, for
5 example, HIPAA, the health information protection laws,
6 or the GLBA, those types of situations, and they exempt
7 that business from complying with the right of request to
8 delete.

9 There's also the issue of verification. So when a
10 consumer makes the request to delete, they must make a
11 Ver -- they must be -- the request must be verified. So
12 the business must take efforts to ensure that the
13 consumer who's making their request is the same consumer
14 about whom the personal information sought to be deleted
15 is about, and if you can understand that there is a
16 concern for security that people can't just go around
17 deleting things of other consumers without their
18 permission.

19 Now moving forward, the next right, which is the
20 right to know -- not sure exactly where to go on here.
21 Try this again. The right to know is basically a right
22 that the consumer has to ask all businesses that
23 collected personal information about them the following
24 things. They can ask for the categories of personal
25 information collected; categories of sources from which

1 personal information is collected; business purposes for
2 collecting, selling, and sharing personal information;
3 and categories of third parties with which the personal
4 information is shared.

5 Another important part is that this request allows
6 the consumer -- this right allows the consumer to ask of
7 the business specific pieces of personal information that
8 has been collected about them. So this is not just a
9 general topic. So for example, if you're talking about a
10 category of personal information, it may be browsing
11 history, but the specific piece of personal information
12 may be the specific links or specific website links that
13 the consumer has interacted with.

14 Now, again overlaying this with the previous
15 presentation, the consumer has this right with regard to
16 both the business that the consumers expects to interact
17 with as well as third parties, such as data brokers.
18 There's also the ability to find out this information
19 from service providers, but again, that would be through
20 the first party that they -- that the service provider is
21 servicing.

22 And again, from our experience, there are some
23 barriers that consumers are commonly faced with with
24 regard to exercising this right, specifically
25 verification again. As you can imagine, there is likely

1 to be some type of security risk if this information
2 about specific pieces of personal information is
3 collected going to the wrong person. And again, there's
4 also certain exceptions to the CCPA when the personal
5 information is governed by other laws such as GLBA,
6 HIPAA, et cetera.

7 Now, touching briefly upon this right, it doesn't
8 particularly, you know, seem to overlay with the data
9 flows exactly, but I do want to mention it. There is a
10 right to equal service, and that basically means that a
11 business cannot discriminate against the consumer because
12 they exercise their CCPA right, and discrimination cannot
13 take a form -- can be seen as denying goods or services
14 to the consumer, charging or providing different rates or
15 quality of good or services.

16 There is an exception. The -- you know, there is
17 the added part, which services can be denied or charged
18 at a different rate if the different level or quality is
19 reasonably related to the value provided to the business
20 by the consumer's data.

21 Now moving on, the right to opt out of sales is
22 probably one of the hallmarks of the CCPA. Basically,
23 the consumer has the right to tell all businesses that
24 sell personal information to stop the sale of personal
25 information. No verification is needed, and the

1 definition of sale is really rather broad. It includes
2 basically any kind of making available of personal
3 information to another business or third party for
4 monetary or other valuable considerations. It does not
5 have to be monitored. It could take the form of
6 discounted services, or free services, for that matter.

7 The right to opt out or fail also requires the
8 provide a "Do not sell me personal information" link on
9 its website, and it's -- there's a uniqueness to it
10 because the opt out applies to consumers that are sixteen
11 years or older, but for those who are under sixteen years
12 of age, it is an opt-in requirement.

13 Now, overlaying this again with the previous
14 presentation discussed, this right is available with both
15 first parties, you know, the business that the consumer's
16 interacting with, as well as third party, data brokers,
17 and that sort. With regard to service providers, this
18 right to does not prevent -- does not prevent the first
19 party from sharing personal information with a service
20 provider because sharing information with a service
21 provider is considered outside of the definition of sale,
22 but to note, service provider is defined strictly in the
23 statute. There are certain requirements in order for a
24 service provider to be an actual service provider
25 recognized by the CCPA. There must by a contract in

1 place; that contract must specifically state that the
2 personal information will only be used to service the
3 business and cannot be sold. It's also made clear in the
4 CCPA regulations that our office promulgated that a
5 service provider cannot use personal information from one
6 business to service another business, except in limited
7 circumstances related to fraud and that sort of thing.

8 So essentially service providers, when receiving
9 personal information, if they are also servicing other
10 businesses, would have to silo that information so that
11 it's -- they can ensure that that information is only
12 being used for the business for whom they are the service
13 provider. And if a service provider does not -- or if a
14 service provider does not comply with the requirements
15 under the law, they are not a service provider, and
16 likely the business is selling personal information to
17 that pseudo service provider.

18 Again, from our experience and from consumer
19 complaints, there are some con -- there are some barriers
20 that consumers may commonly face with regard to the
21 exercising of this right. Sometimes businesses are not
22 clear with regard to their representation that they do
23 not sell personal information when in fact they do.

24 There's also an issue where even though this right, no
25 verification is needed to exercise this right, oftentimes

1 businesses may require some type of verification
2 because -- yes.

3 And while identification may be allowed, questions
4 basically asking the consumer questions in order to allow
5 the business to figure out whose information is whose, we
6 often see abuses in this case area. And also another
7 commonly seen barrier would be the fact that the
8 requirement under the CCPA is that a business is only
9 required to disclose categories of third parties with
10 whom they have shared or sold personal information with.

11 So oftentimes, a consumer who makes this right to
12 opt out of sale request of the business, they don't know
13 who else that business has sold personal information to.
14 So there's no way to go down the stream and ensure that
15 people -- that the first party business sold personal
16 information to also honored the consumer's right under
17 the CCPA. This somewhat changes under the CPRA.

18 The issue here is that, you know, one way in which a
19 consumer may be able to exercise this right with a bunch
20 of third parties who have information about them is to go
21 through our data broker registry on the California AG's
22 website. However, unfortunately there are so many data
23 brokers already registered on the data broker registry,
24 currently it's 450 data brokers, it makes it very
25 difficult for a consumer to be able to exercise their

1 right to opt out of the sale for many businesses at once.

2 Now, the CPRA amendment to the CCPA added this
3 concept of right to opt out of sale or sharing. This --
4 you know, the definition of sale was broad already and
5 may have already addressed many of the situations that
6 are now covered under this new term of opt out of
7 sharing, but one of the issues were that it usually
8 required some type of factual inquiry with regard to
9 whether or not there was consideration for the sharing,
10 whether or not those with whom the information was shared
11 were considered service providers or not.

12 So this amendment of the CPRA added this language
13 regarding share so that sharing means any sharing of
14 personal information for the -- for cross-contact -- for
15 cross-contact behavioral advertising, whether or not for
16 monetary or other valuable consideration. So while this
17 may have already been covered under the original right to
18 opt out of sale, this amended language just makes it all
19 the more clear.

20 Again here, there is no service provider exception
21 for cross-contact behavioral advertising, so there's no
22 instance in which a business can say, oh, I am using this
23 service provider and sharing information with this
24 service provider to provide me cross-contact behavioral
25 advertising or personalized ads. That is not something

1 that can be done or done in this instance. All other
2 parts are relatively the same. No verification is
3 needed, a link is required on their website, and there is
4 an opt-in requirement for those under sixteen years of
5 age.

6 Overlaying this with what the previous presentation
7 discussed, you know, this very clearly addresses issues
8 of real time bidding or online behavioral advertising,
9 and in this instance makes clear that a business must
10 give an option to consumers to not share personal
11 information for these purposes.

12 Now, another right that has been added by the CPRA
13 amendment were -- is this right to correct. Now, the
14 right to correct applies to inaccurate personal
15 information maintained by the business, and a business
16 must -- shall use commercially reasonable efforts to
17 correct the inaccurate information. Other than that, the
18 CPRA amendments very specifically state that the
19 regulations will flesh out the details of how this right
20 is operationalized.

21 Now, overlaying this again with the previous
22 presentation with regard to data flows, this right to
23 correct under the law certainly addresses first-party
24 situations, so the business in which the consumer intends
25 to interact with, as well with third parties such as data

1 brokers, and again with regard to service providers, only
2 through the first party that they're interacting with.
3 And in this -- and the law also states that verification
4 is required with regard to this right to correct.

5 Now, next we have the right to limit. The right to
6 limit the use and disclosure of sensitive personal
7 information is basically a right where a consumer can
8 tell a business to only use sensitive personal
9 information about them for what is necessary to provide
10 the good or service that the consumer expects, with some
11 minor exceptions.

12 Sensitive personal information is basically a subset
13 of personal information and includes things like health
14 information, financial information, Social Security
15 number, as well as information about protected classes,
16 such as the consumer's right or sexual orientation or
17 information about their sex life, that sort of a thing.
18 So with regard to that subset of personal information
19 that has a higher -- that people -- you can imagine why
20 it would be more disconcerting for that information to be
21 proliferated about the consumer in the marketplace, there
22 is this additional right where the consumer can limit the
23 business's use of that personal information to only what
24 is necessary to provide the good or service that the
25 consumer expects and some limited exceptions.

1 Those limited exceptions, you know, are generally
2 tied to consumer expectation, what is necessary and
3 proportionate. There's some exceptions for public goods,
4 for example, with regard to security and fraud
5 prevention, safety of people, quality and safety of
6 goods, and then also some exceptions for uses that aren't
7 quite as offensive, such as, you know, non-personalized
8 ads and internal business uses or warranties, that sort
9 of thing.

10 Now again, overlaying this with what our previous
11 presentation discussed, this right to limit applies to
12 both the first party, the consumer, the business the
13 consumer is expecting to interact with, third parties as
14 well, and then service providers through the first party,
15 and in -- with regard to this right, no verification
16 again is needed.

17 Finally, I wanted to address a new -- it's not per
18 se a right as it is as a requirement, a data minimization
19 and purpose limitations on a business. It's restrictions
20 placed upon the business with regard to the collection,
21 use, and retention and sharing of personal information.
22 The collection, use, retention, and sharing of personal
23 information by the business has to be reasonably
24 necessary and proportionate to achieve the purposes for
25 which the personal information was collected or processed

1 or for a disclosed purpose that is compatible with the
2 context in which the personal information is collected.

3 You know, now with regard to the CPRA amendments, a
4 contract is now required for all sales and sharing of
5 personal information, and the business has to specify a
6 purpose with regard -- within that contract, and it
7 obligates the third-party service provider or contractor
8 to comply with the CCPA. It also -- the contract is also
9 supposed to include certain right by the business to
10 ensure the compliance with the contract.

11 Now -- but overlaying this with what the previous
12 presentation discussed, this is a fundamentally -- this
13 is fundamentally different than how businesses have been
14 operating thus far. Previously a business could
15 generally do anything with adult personal information or
16 personal information of consumers above the age of
17 sixteen as long as it was disclosed properly to the
18 consumer, but now there's limitations. Even if you
19 disclose what you're going to do, it cannot be reasonably
20 necessary, proportionate, or compatible with the context
21 in which the personal information was collected.

22 So the new question to ask with regard to these data
23 flows of where your personal information is going would
24 be would a consumer expect the business to use the
25 personal information for this purpose, is it reasonably

1 necessary and proportionate for the sharing of that
2 personal information or that data flow, and is it
3 compatible with the consumer's expectation. This
4 interacts with again the notice of collection that I had
5 mentioned previously, which is a required disclosure to
6 the consumer. So now that notice of collection has to
7 take into account whether or not, you know, the purpose
8 and use of the information is reasonably necessary,
9 proportionate, and to achieve the purposes of which the
10 personal information was collected.

11 So the -- you know, this is a lot of information, I
12 imagine, and I have to say that this presentation is not
13 exhaustive of all the things that are included in the
14 CCPA as well as the CPRA amendments. There are a lot of
15 nuances to this law, but I hope this presentation gives
16 you a better understanding of how the CCPA applies to
17 data flows. Thank you.

18 **MS. URBAN:** Thank you very much, Ms. Kim. Much
19 appreciated that you were willing to take the time to
20 walk us through all of that. So thank you, and thanks
21 again just generally to both of your first two speakers.

22 We are running actually about five minutes ahead of
23 schedule, which is great, and we're going to go ahead and
24 take our lunch break. Our lunch break will go until 1
25 o'clock p.m. We'll reconvene at 1 o'clock for the

1 afternoon's presentations. Please feel free to leave the
2 video or teleconference open or to log out now and back
3 in at 1 p.m. It's up to you. So with that, we will
4 start our lunch break, and see you all at 1 o'clock.

5 (Whereupon, a recess was held)

6 **MR. GOURLEY:** Okay. Looks like we're recording, and
7 you should be ready to go.

8 **MS. URBAN:** Thank you very much, Mr. Gourley, and
9 everyone, welcome back to the California Privacy
10 Protection Agency's March 2022 pre-rulemaking
11 informational sessions. I would like to remind everyone
12 that we are recording this meeting.

13 If you're just joining us, we are listening to a
14 series of presentations, which you can find under agenda
15 item 2 on your schedule, an "Overview of Personal
16 Information and the California Consumer Privacy Act."

17 We've had two presentations this morning, and we
18 have four more to come this afternoon, and then we will
19 finish the day with public comment. I'll remind everyone
20 how to engage in public comment when we get to that part
21 of the day. Please all note that we may also take a
22 short break at some point, not as long as lunch, but keep
23 an eye out for that. And if you have to step away, again
24 we're recording, we'll have transcripts, and the slides
25 that, if people used them, will be available once we can

1 get them processed and up on the website.

2 So we will now continue with our first set of
3 informational presentations. If you're following along,
4 we're on day 1, agenda item 2, part C, "Business and
5 Consumer Interactions: Dark Patterns."

6 I am delighted to introduce two experts on this
7 topic. Dr. Jennifer King is the privacy and data policy
8 fellow at the Stanford University Institute for
9 Human-Centered Artificial Intelligence. An information
10 scientist by training, Dr. King's research is at the
11 intersection of human computer interaction law and the
12 social sciences. Her work examines the public's
13 understandings and expectations of online privacy as well
14 as the policy implications of emerging technologies.

15 She has recent work on notice and choice,
16 California's privacy laws, and dark patterns. She has
17 served as a member of the California State Advisory Board
18 on mobile privacy policies and the California State RFID
19 Advisory Board, and I'm going to pause here and say that
20 RFID is for radiofrequency identification, because that's
21 a rule in my classes at the university.

22 Previously Dr. King was the director of consumer
23 privacy at the Center for Internet and Society at
24 Stanford Law School from 2018 to 2020. Before coming to
25 Stanford, she was a codirector of the Center for

1 Technology, Society, and Policy at UC-Berkeley and was a
2 privacy researcher at the Samuelson Law, Technology, and
3 Public Policy Clinic at Berkeley Law. Dr. King holds a
4 doctorate in information management and systems from the
5 University of California-Berkeley School of Information.

6 And our second speaker on the topic is Professor
7 Lior Strahilevitz.

8 Hi, Professor Strahilevitz. Thank you for joining
9 us.

10 He is the Sidley Austin professor of law at the
11 University of Chicago, where he has taught since 2002.
12 Professor Strahilevitz's research interests include
13 privacy law, property law, consumer contracts, and law
14 and technology. He is a member of the American Law
15 Institute and has served as deputy dean of the University
16 of Chicago Law School. Professor Strahilevitz has
17 authored or coauthored nine books and dozens of
18 law-reviewed articles. He is a graduate of the
19 University of California-Berkeley and the Yale Law
20 School.

21 And with that, I will turn things over to Dr. King.
22 I believe you are first, but you and Professor
23 Strahilevitz can organize the information however you you
24 like, and thank you very much for being here.

25 **DR. KING:** Thank you, Chairwoman Urban. Okay. I'm

1 going to share my screen. Give me one second because I'm
2 going to draw a box around my slides and move this out of
3 the way. It takes me one second here. Oh, come on,
4 Zoom. Sorry. This is just how I deal with PowerPoint.
5 Okay. Can everybody see that? I hope so, because I
6 can't see any of you.

7 **UNIDENTIFIED SPEAKER:** Yes, we can.

8 **DR. KING:** Thank you. Okay.

9 So I'm Dr. Jen King. So I'm from Stanford HAI,
10 although I need to note that I am speaking for myself and
11 not for Stanford or HAI in my remarks today.

12 So I'm going to talk about dark patterns. Very
13 quickly -- I'm sorry. There we go. Let me just set my
14 timer.

15 Okay. So I'm going to go quickly over the
16 definition of what dark patterns are; where we find them;
17 how they actually do their work; the difference between
18 things that persuade versus manipulation, coercion, and
19 deception; some types of dark patterns; and show you some
20 examples. And I'll move pretty quickly, as Lior will
21 speak after me in more detail in his specific research.

22 Okay. So let's start. So what is a design pattern?
23 So when we talk about dark patterns, the pattern part is
24 something called a design pattern. The example on the
25 slide are examples of toggle switches.

1 So this is a form of design pattern, basically a
2 building block that online designers use to build mobile
3 apps and web pages. They're reusable components that we
4 use over and over again that comprise the different parts
5 of the interaction design, the way we interact with user
6 interfaces, those things we -- we look in the websites
7 and mobile apps and so on.

8 And so when we talk about dark patterns, what we
9 find right now is that the research community has really
10 only been looking at dark patterns pretty closely for the
11 last five years. And so there isn't a single definition,
12 necessarily, that everybody is completely coalesced
13 around. So I'm going to go through a couple here.

14 But what we're talking about, starting with Harry
15 Brignull's definition -- Harry created the first dark
16 patterns website, darkpatterns.org. It's a great
17 resource if you'd like to learn a little bit more about
18 dark patterns.

19 He's called them a user interface that has been
20 carefully crafted to trick users into doing things. They
21 are not mistakes. They are crafted with a solid
22 understanding of human psychology, and they do not have
23 the user's best interests in mind.

24 And then Lior, in his work that he'll be presenting
25 after me, he's called them techniques that manipulate

1 users to do the things they would not otherwise do.

2 Another definition that I like a great deal comes
3 from colleagues at Princeton, where they've looked across
4 all the different ways that people have described dark
5 patterns, and they've defined them as user interface
6 designs choices that benefit an online service by
7 coercing, manipulating, or deceiving users into making
8 unintended and potentially harmful decisions.

9 So the idea here is that a dark pattern is something
10 in an interface that essentially gets you to do something
11 that you didn't plan to do or didn't necessarily want to
12 do. And so I'll talk more about that as we go through.

13 So first, the reason why this is relevant today is
14 both the CCPA and the CPRA have references to dark
15 patterns. So in the CCPA there is specific text that, in
16 terms of describing those do not sell opt-outs that you
17 may have heard about earlier today, there's language that
18 basically tries to prevent different forms of dark
19 patterns in those opt-outs to make sure that when people
20 are opting out, they are given a clear way of doing so
21 and not presented with an interface that makes it
22 difficult for them to enact with those opt-outs.

23 The CPRA actually includes a specific definition of
24 dark patterns, which is a user interface designed or
25 manipulated with the substantial effect of subverting or

1 impairing user autonomy, decision-making, or choice as
2 further defined by regulation.

3 And it's specific to consent interfaces right now in
4 the way that the statute was put before the voters. And
5 so when we talk about dark patterns right now in the
6 CPRA, they've been very narrowly focused in terms of
7 consent and the -- basically the touchpoints were we, as
8 individuals, consent to give up personal information
9 online.

10 And so there is some momentum right now to actually
11 move away from the term dark patterns for two reasons.
12 One is that actually a number of people are actually
13 quite confused about the use of the term patterns, just
14 not having any background in the kind of user human
15 computer interactions face, such as I have.

16 And so there's that piece of it, but then there's
17 also concerns about the unintended implications of the term
18 dark. And so some of the ideas that have been proposed
19 are to say deceptive or unfair design patterns or to use
20 manipulative or deceptive design as a term. There really
21 isn't kind of a common agreement yet. I will use
22 manipulative design throughout this presentation.

23 But one of the problems with this right now is that
24 the term dark patterns has already been written into
25 legislation and -- including the CPRA, for example. It

1 also has -- the word deception, in particular, has very
2 specific legal meanings, and which I actually will define
3 a little bit later.

4 And so calling it deceptive patterns, for example,
5 may make sense in a research context, in a casual
6 context, but in the legal context that may actually be
7 somewhat misleading. And we're still at this point where
8 people are trying to figure out, you know, where to go
9 with this. But I just want to raise that upfront.

10 Okay. So context. Where do we find deceptive
11 designs and dark patterns? And so right now there are
12 three primary contexts that we see them. So we see them
13 in online shopping and e-commerce, where people
14 essentially experience usually a loss of income -- or not
15 income, but they lose money as a result of dark patterns
16 or they may experience price discrimination.

17 In the privacy space, in terms of disclosure and
18 consent, where people are forced to give up more personal
19 information than they would desire or forced to consent
20 any personal information in cases where they may not
21 actually want to do that at all.

22 In the gaming and gambling spaces, we have what we
23 call addictive dark patterns or attention-based dark
24 patterns. And those are the things that -- people find
25 very hard to stop an activity once they're engaged in it,

1 and so that's a space where I would call it more
2 emergent. There's more research needed to really know
3 how to understand that space.

4 Predominantly, though, we're seeing them in these
5 e-commerce contexts. And where you find them
6 specifically are at these places I call decision points.
7 And those are places where, as an individual, you're
8 making some kind of decision or you're executing an
9 action.

10 So you're deciding between two buttons, for example.
11 I consent or I don't consent. That's a decision point.
12 You know, before you hit "I agree" in a terms and
13 conditions acceptance or before you make an online
14 purchase. Those are all kind of decision points where we
15 most often see dark patterns show up.

16 Okay. So how do these actually work? And so this
17 is an interesting issue. So we think that in general
18 what they -- the way they succeed is that they are using
19 kind of two flaws in how humans think: something we call
20 heuristics, which are mental shortcuts, that we all use
21 as a way to kind of make decisions easier for us to make,
22 as well as cognitive biases, and these are demonstrated
23 systematic errors in the way we think.

24 There's a couple things I want to kind of comment on
25 first before I go on in this one, which is first that a

1 lot of this work comes out of the field of behavioral
2 economics, and it works under this assumption that
3 there's this kind of perfect rational consumer.

4 And so we all know that no one -- maybe with very
5 few exceptions -- is a perfect rational being. And so a
6 lot of what we're documenting are, you know, what I think
7 most of us would consider are normal errors in the way we
8 think or, you know, just kind of, you know, normal things
9 in the course of our everyday lives, because none of us
10 is kind of a perfect rational being.

11 Second, the most of this research has been done
12 within the kind of U.S. and European Western tradition.
13 And so while we assume that they are global, there really
14 hasn't been much contextual research or cross-cultural
15 research in this area. And so, you know, I say that with
16 basically big caveat, that, you know, we don't know
17 necessarily if these are, in fact -- are all of the
18 things we call biases and heuristics are necessarily, you
19 know, globally experienced.

20 But certainly, within our society, we have
21 demonstrated that they exist. And I'm not going to go
22 into them in detail, but just to note that, you know,
23 there are examples such as the availability heuristic.
24 And that's one where you often make a decision based on
25 what the -- the most recent piece of information that

1 you've been exposed to.

2 Or something like hindsight bias, where you think
3 back over an event and the type of thing that you're --
4 that you're referencing or the information you're
5 referencing kind of makes it seem as if that you knew
6 that information all along, yet it may have been
7 something that only, you know, came apparent to you after
8 an actual event occurred.

9 And so this space has been influenced -- or dark
10 patterns have been influenced both by research in this
11 space, but also through the work by one of my Stanford
12 colleagues, B.J. Fogg. And B.J. Fogg is kind of the --
13 I'd probably call him the father of what we call
14 persuasive design.

15 And so his work in the early '90s -- or mid-'90s to
16 the early 2000s really began to focus on what is it
17 that -- how can we generate websites or how can we design
18 ways of interacting online that really persuade people,
19 that make it easy for you to decide to sign up for
20 something or to stay engaged with something.

21 And so there's this whole field of persuasive design
22 that has really contributed to the -- kind of the
23 introduction of dark patterns because, as we have seen,
24 things that can be used to persuade can also be used to
25 potentially deceive.

1 We also have seen kind of a counter movement in
2 things called nudges, for example, where, you know, the
3 focus there is to try to nudge people into making
4 decisions that act in their best interests.

5 So one of the classic examples in this space is the
6 idea that, you know, you may have a job that
7 automatically enrolls you in a 401(k) retirement savings
8 plan, rather than making it dependent on you to sign up
9 because it's in your better interest to go ahead and be
10 enrolled in something like that than to have to take the
11 effort on your own to enroll in it.

12 And so it's these kind of positive nudges, these
13 things that we see try to help people make good decisions
14 end up being hijacked to help you -- help you make
15 decisions that -- more in the best interest of the
16 company that is producing them, rather than you.

17 Okay. So I'm going to pause for a second and talk
18 about digital dark patterns just to give you an analog to
19 what dark patterns in kind of the physical space. And so
20 the example I have here, this is something called a
21 planogram, and this is a planogram of a grocery store.

22 And just to kind of illustrate the similarities
23 between kind of these physical built environments in the
24 online space is to note that when you go into a large
25 grocery store -- and I -- you know, I'm talking a major

1 grocery store, not your corner market -- what you'll find
2 is that that entire space has been very carefully
3 designed from top to bottom, from the point of view of
4 not only everything in terms of the aisle placement, but
5 literally everything on the shelves. And marketers pay,
6 you know, tremendous amounts of money to place their
7 products at particular places in that grocery store.

8 And so as a consumer, what you may do is you may
9 walk into a grocery store and decide you need something
10 like a gallon of milk, probably one of the most common
11 purchases people make, especially if they're in a hurry,
12 but you'll find is that more often than not, that milk is
13 going to be located at the back of the store.

14 And why is that? It's because the store has been
15 designed to kind of optimize the idea that for people who
16 need to come in and buy just a couple of, you know, kind
17 of staple goods, the things you need all the time, we're
18 going to force you to walk through the entire store so it
19 increases the likelihood that you're going to pick up a
20 product as you walk through.

21 And so, you know, online environments are very
22 similar in that way in that they are completely designed
23 spaces. You know, there's nothing accidental about them.
24 Everything about them has been planned from top to
25 bottom. And so your journey through that space has been

1 very carefully designed.

2 Of course, in a supermarket, you know, you're not
3 forced to walk down a particular aisle, but again, the
4 entire experience has been optimized to try to get you to
5 potentially pick something up as you walk through so that
6 you walk out with more items than you intended to
7 purchase when you walked in.

8 And so as it happens here in -- I'm a resident of
9 the city of Berkeley, and in Berkeley we have one of the
10 first laws, I think, in the nation that has attempted to
11 actually counter that type of persuasive design, and
12 that's by eliminating all sweet junk foods and such at
13 the checkout aisles.

14 I'm actually not sure if this has potentially been
15 enforced yet, but just to say that, you know, there's
16 this sense that even in these built environments that
17 this type of persuasion is meaningful, it works, you
18 know.

19 And especially if you're somebody with a small child
20 and you go grocery shopping, you have that sense of
21 things just being automatically added to your grocery
22 basket as you walk through. At least, that's what
23 happens to me.

24 And so just to say that, you know, even in the -- in
25 the shopping context, the market context, you know, there

1 are forces at work that -- or deliberate decisions at
2 work to really persuade you into making particular
3 purchases.

4 The one thing, though, that we don't have
5 necessarily is you're not going to leave the grocery
6 store -- again, unless you have a small child tagging you
7 like I do -- with extra things added to your cart, and
8 yet that is one of the examples that we see in the
9 e-commerce space, that people will actually checkout of
10 an online merchant and find that they've been enrolled in
11 a program that they didn't necessarily sign up for or
12 didn't affirmatively sign up for or even as far as having
13 things added to their cart or added to a service in terms
14 of extra fees that they just -- that weren't disclosed at
15 the beginning and suddenly they're there by the time you
16 get to the checkout.

17 As a sidenote, I will note that I think we are
18 beginning to see dark patterns in these kind of physical
19 spaces as well, not just on screens, but actually on
20 screens in these places.

21 Just this morning my husband took a trip to a local
22 large pharmacy chain, and at the credit card terminal was
23 presented with a screen that gave him two options, either
24 to accept that the pharmacy would send him text messages
25 or to print info, which was a choice that basically gave

1 him a printed slip from the register that made it unclear
2 whether he was actually now enrolled in the program or if
3 it was -- they were going to actually -- you had to
4 follow the instructions on it to unsubscribe from these
5 text messages.

6 So just to point out that this is a phenomenon
7 that's becoming very widespread, and not just again on
8 mobile apps, mobile devices or online, but potentially
9 also in real life checkout screens.

10 Okay. So what types of dark patterns are there? So
11 let me go through these very quickly. So first we have
12 kind of two general areas of dark patterns. First we
13 have those that modify the decision space, and those are
14 the ones that either remove options that maybe you would
15 have wanted, you know, things that make it harder to
16 actually make that decision versus those that manipulate
17 the information flow. And those are the ones that
18 potentially kind of don't disclose to you everything that
19 you should know in order to make a very, you know, well-
20 reasoned decision.

21 And so things that we see that modify the decision
22 space are what we call asymmetric, you know, patterns
23 that essentially emphasize choices that benefit the
24 company over a choice that benefits you, such as if you
25 hit -- see a screen with a big green "I accept" button

1 and a link in very small letters that say maybe "I don't
2 accept". You know, that's an asymmetric interface. It's
3 emphasizing one choice over the other.

4 There are covert ones, which essentially try to
5 steer you towards making a purchase or a decision without
6 all the knowledge you need. So hidden fees, I think, are
7 a good example of that.

8 Restrictive interfaces, where, you know -- and I'll
9 have an example of that in just a couple moments, where
10 you're given an accept button, for example, on a
11 condition, but no way to reject it, only the accept. So
12 your options are restricted.

13 Then in the world of kind of manipulating the flow
14 of information to you, you have those that will kind of
15 hide or steer the information that you need in order to
16 make a decision. Maybe it's there, but you have to, you
17 know, try to hunt for it.

18 We famously see these with privacy policies, the
19 fact that there's, you know, maybe information that you,
20 as a consumer, was interested in but it's buried in, you
21 know, 5,000 words of a privacy policy that you would have
22 to hunt through.

23 And then we have outright deceptive interfaces, so
24 things that -- as I'll define in a little -- in a
25 moment -- that actually kind of produce false beliefs,

1 things that are essentially lies, that are misleading you
2 actively.

3 Okay. So let me dig into a little of the
4 differences between persuasion versus deception,
5 coercion, and manipulation. Okay. So persuading is when
6 we really appeal someone directly to make a decision.

7 And so, you know, this is me potentially -- or I
8 would say most advertising falls under this category.
9 You know, if you're flipping through a magazine, you see
10 an ad, you know, that's persuasive interaction.

11 They're trying to get you to buy the shoes, to book
12 the vacation, what have you, but it's -- you know, it's a
13 fairly straightforward interaction. And, you know, it
14 might be appealing to you or it may not. You know,
15 that's kind of the mystery of advertising, if you want to
16 put it that way.

17 Deception is actually the planting of false beliefs.
18 Okay. So this is a very specific meaning where the
19 practice, basically, is you've been lied to or you've
20 been misrepresented to. You know, the diet pills say
21 you'll lose 20 pounds and you don't lose any pounds. You
22 know, it's that type of misleading information.

23 Coercion is when we constrain your options and so
24 that essentially the only kind of logical way forward for
25 you when you're being coerced is to end up making the

1 decision that the coercing party wants you to make.

2 I think a lot of dark patterns fall under this
3 space, where you're not exactly prevented sometimes from
4 making a choice, but it's clear that the easiest way
5 forward is to just do what the company wants you to do.

6 And then we have manipulation. Manipulation is more
7 of this hidden influence. Okay. And so this is when
8 somebody is trying to get you to do what they want you to
9 do, but they're not being very obvious about it. They're
10 potentially, you know, exploiting your vulnerabilities.

11 And this is an area, I think, of a special concern
12 to us in the privacy space, given the information
13 asymmetry between most of us and advertisers and large
14 platforms, that a company could have enough information
15 about you to try to understand, you know, Jen (ph.) is
16 much more of a -- you know, she seems much more inclined
17 to buy things after 10 p.m. than somebody else, and so
18 we'll show her ads, if she's online after 10 p.m., you
19 know, with, you know, particular things that we think,
20 you know, make her more, you know, willing to buy, just
21 as an example.

22 Okay. So may I just mention very quickly, in terms
23 of, like, trying to understand dark patterns from a
24 consumer's perspective or if you're looking to actually
25 report your own experience with dark patterns, I along

1 with some colleagues at Stanford, at the Digital Civil
2 Society Lab, have taken over the website
3 darkpatternstipline.org.

4 It's a public resource. There are examples there,
5 and people can actually go and report their own
6 experiences with dark patterns to the tip line as well.
7 I'll just note that if you do so, please, please, please
8 include a screenshot, because otherwise it's very hard
9 for us to verify them.

10 Okay. So how did we get here with dark patterns?
11 So one of the biggest reasons that we've been able -- or
12 that the dark patterns have been able to proliferate has
13 been something called A/B testing. And this is the
14 ability of companies to test interfaces at an incredibly
15 large scale.

16 You know, as a researcher, speaking for myself, if I
17 wanted to do some type of user test, I would have to go
18 recruit, you know, mostly likely a group of, let's say,
19 twenty or fifty Stanford undergraduates and pay them and
20 try to do some kind of small-scale test.

21 But if you're a large platform or even just a, you
22 know, decent sized company, you now have the ability to
23 do these kind of A/B tests at scale with thousands and
24 thousands and, in some cases, millions and millions of
25 customers.

1 And so this allows you the ability to really refine
2 interfaces and try to find the ones that lead to the most
3 conversions, you know, the most sales, the most
4 memberships, whatever it might be.

5 And so the example here on this slide -- you know,
6 there are two interfaces that are for the same website,
7 interface A, interface B, and they show you that in the
8 graph, you know, 23.7 percent of people converted when
9 they saw interface A.

10 And so through this kind of large-scale A/B testing,
11 companies have really been able to pick up on precisely
12 the types of things that kind of push people over the
13 edge in terms of what gets them to sign up for something
14 and what doesn't.

15 Okay. So now I'm going to walk through a handful of
16 examples, and then I'll hand it over to Lior for his
17 piece. So this is a deceptive type of dark pattern
18 called false urgency.

19 And so this again, mostly we see this in the
20 e-commerce context. And what it's acting on is this idea
21 that time is running out, you know, which is something,
22 you know, we see a lot in -- in the sale sphere. You
23 know, act now, limited time offer.

24 You know, the versions of that we see online are,
25 you know, when you get basically a countdown timer,

1 you're told, you know, eight other people are looking at
2 this right now, you'd better act, and so on.

3 And so one of the things that researchers have found
4 in many cases is that often these timers are completely
5 fictional. And so you actually look at the code for the
6 website, if you just hit refresh, you know, the timer
7 will start over. It's not actually tied to any kind of
8 realistic analytic system, for example.

9 That's not always true, but it has been largely
10 true. And so, you know, especially when those are
11 completely fictional, it's absolutely -- we consider them
12 a dark pattern.

13 Okay. A content-based dark pattern is something we
14 call guiltshaming or confirmshaming. This is a fairly
15 wide experience. Most of you probably have experienced
16 something like this, you know, where basically you're
17 being guilted or kind of shamed into making the choice
18 you want to make.

19 I actually find these to be remarkably effective,
20 even in my own life, even though I work in this area,
21 because sometimes it just makes me stop and have to sit
22 there and think, wow, am I really a bad person to click
23 this link?

24 I mean, yes, I know I'm not a bad person to click
25 the link, but it makes you stop and think. And so this

1 is kind of a form of harassment through guilt that we see
2 repeatedly in this space, especially when people are
3 unsubscribing to a service.

4 Okay. This is another thing called nagging, again,
5 another form of harassment, where essentially you're just
6 repeatedly asked to agree to something, even maybe after
7 you've said no, I don't want to do it, which, I think,
8 the buttons here are a good example of that.

9 Your choices are "maybe later" or "okay". You know,
10 maybe later, kind of implying that the door is left open,
11 you haven't said no, but maybe if I keep asking you over
12 and over again, you'll just say yes.

13 This is a content-based dark pattern with confusing
14 double negatives, so where, again, you're using language
15 to describe something in a way that's unclear and
16 misleads people. Do you wish for your record not to be
17 sent to my health record?

18 You know, what is the answer to that? You know, is
19 no -- does no mean yes or does yes mean no? And so
20 that's the type of thing that makes people have to really
21 stop and think and grapple with what's being asked of
22 them. And there is absolutely no reason to phrase
23 anything that way. You can, you know, always make it
24 much more clearer than that.

25 Obstruction. So again, this is a way of kind of --

1 of coercing you and preventing you from making the choice
2 you want to make. So these are just examples. Actually,
3 the one on, I think, your right -- I apologize if that's
4 not correct -- we offer several ways to cancel your
5 subscription.

6 You know, that's an example that we see commonly,
7 where signing up for something is quite easy. It takes a
8 couple clicks; you're subscribed. And then if you want
9 to cancel a service, guess what, you have to chat with a
10 customer service agent, you have to get on the phone.
11 There's no simple just "cancel my account" click. That's
12 something that's extremely common and obviously puts a
13 lot more load on you, as the consumer, to have to grapple
14 with that than it would otherwise.

15 Okay. So dark patterns in terms of the consent
16 space. And so -- I apologize. I'm going to take a quick
17 swig of water.

18 Okay. So all of us have probably seen cookie
19 consents or opt-out -- different terms of opt-out
20 consents. You know, these are often confusing. Or in
21 the example of the blue one on the screen, you know,
22 you're given a single choice, that's to accept. You know
23 what is your choice otherwise? Probably to close the
24 browser or close the app and walk away. So it's
25 basically take-it-or-leave-it situation.

1 You know, same with the example on the bottom. Your
2 only option is yes, I want to continue to see relevant
3 ads. No, I don't want to see ads. It's just not even
4 given to you.

5 The other one on the screen I included just because
6 it is extremely confusing. You know, you're given the
7 opportunity to probably reject all cookies, accept all
8 cookies or and then just accept. It's just unclear
9 exactly how to even navigate that particular set.

10 Relevant to us here in California and the CCPA are
11 the do-not-sell requests. I don't know if any of you
12 have potentially tried to make do-not-sell requests, but
13 one of the things we have been observing is that often
14 they're being implemented using toggle switches, and that
15 the state of those toggle switches is often extremely
16 unclear.

17 That it's not -- you know, if you go through these,
18 it's not clear whether if you turn the toggle switch to
19 on versus off, whether you've actually agreed to opt out
20 or not. And so that's a dark pattern we've seen
21 repeatedly in this space.

22 Okay. So my last slide, and I think I'm just at
23 time. What are some of the open policy issues in this
24 space? So what I would just note is that with the CPRA,
25 the current scope is really framed tightly around

1 consent, but I think that there is an opportunity there
2 to rethink consent standards within that space.

3 And that's something I talk about in a paper I wrote
4 in the Georgetown Law Tech Review last year, just that I
5 think there's more opportunity not just to really
6 narrowly think about how we consent but more broadly
7 think about how we may consent something a lot more
8 better and effective for people.

9 Within the privacy space especially, I think there's
10 ways to identify areas outside of just consent, where we
11 see privacy manipulative design interact, and such as
12 when we see personal data being used to influence your
13 choices or your decisions.

14 I also want to note that measuring and assessing the
15 impacts of manipulative design requires expertise. And
16 so this is something that the agency, I would argue,
17 really needs to consider as it hires its staff, that you
18 need to have experts on hand who understand these issues.

19 This is outside of the kind of normal law realm of
20 just legal counsel, and that you actually need a way to
21 connect with the public in order to receive complaints or
22 suggestions or reports of dark patterns. I think that's
23 going to be a very vital issue.

24 And then finally, what I have heard often from
25 businesses in this space as I give these talks is that

1 businesses really want to see positive guidance on kind
2 of what to do and what not to do and potential standards
3 around what is acceptable practice when we ask people for
4 choices or to make decisions.

5 And with that, I will stop screensharing and hand it
6 over to Lior. Thank you very much.

7 **MR. STRAHILEVITZ:** Thank you so much, Jen. That was
8 really terrific. And thank you, Jennifer, for the
9 introduction. I'm going to pull up my slides, if Zoom is
10 going to cooperate, which is always, as Jen illustrated,
11 a little bit of an off (ph.). Well, you know what, let
12 me try this. This will put me in the corner of the
13 screen, but I think that actually should work out just
14 fine with these slides.

15 Okay. So it's really a pleasure to be here to talk
16 about some of the research that Jamie Luguri and I have
17 been doing on dark patterns over the last several years.
18 And this will be a sort of data heavy presentation, where
19 I'm able to talk about a lot of the experimental work
20 that we've done, looking at dark patterns, trying them
21 out on ordinary American consumers, and seeing how they
22 respond.

23 So before Jamie and I started researching these dark
24 patterns questions that Jen has really thoughtfully
25 introduced, we had some existing academic research about

1 dark patterns that highlighted their prevalence, their
2 increasing prevalence.

3 These are probably the two best academic papers by
4 teams of researchers in the United States and in Europe
5 that have documented, often through using really creative
6 techniques in computer science, the proliferation of dark
7 patterns and their prevalence, especially on the more
8 far-reaching and successful sites in e-commerce.

9 But knowing that dark patterns is prevalent doesn't
10 necessarily tell you that they work, although it implies
11 that they do, because after all, why would companies be
12 investing a lot of money in shifting over towards dark
13 patterns if they weren't gaining some additional revenue.

14 Yet we were really kind of flying blind with respect
15 to which dark patterns are more effective, which dark
16 patterns are relatively effective, and how effective in
17 general are the kind of cocktails of dark patterns that
18 we often see employed at the websites and in the apps
19 that Jen just illustrated.

20 So to that end, Jamie and I have launched a couple
21 of very large-scale experiments. We're talking about
22 thousands of Americans in our experiments. And what's
23 really important to understand about our research is that
24 we're going to run these dark pattern experiments, but
25 it's kind of like running a Gallup poll or a Los Angeles

1 Times poll.

2 The group of American adults that we're going to
3 expose to dark patterns look just like the United States
4 adult population, or at least the portion of the adult
5 population that has internet access, which is about 91
6 percent.

7 And so it's census weighted, meaning our sample of
8 respondents is going to look just like the U.S. adult
9 population in terms of gender and race and age and region
10 of the country and education level.

11 And that's important both because we can see how
12 dark patterns are operating on, you know, real, everyday
13 people, like you and me, but also, we'll be able to dig
14 into some of the demographics and see whether some groups
15 are more vulnerable to dark patterns than others.

16 So I'm going to talk about a couple of experiments.
17 In the first experiment we began by actually taking about
18 ten minutes of people's time and asking them to answer a
19 whole series of questions about their privacy
20 expectations and their privacy preferences.

21 And then after people answered this battery of
22 questions and also provided some demographic information
23 about themselves, we told them that on the basis of their
24 answers we were calculating their privacy propensity
25 scores.

1 And it turned out, based on their answers, our
2 algorithm had identified them as someone who cares more
3 about privacy than the average person. We told everybody
4 that. Everybody kind of thinks -- just about everyone
5 kind of thinks they care a lot about their own privacy,
6 so that wasn't an especially fishy story.

7 And then we told people, hey, we have good news.
8 We've partnered with the nation's largest provider of
9 identity theft protection, and based on the information
10 you've already given us, we've gone ahead and signed you
11 up for a plan that will protect you against identity
12 theft and loss of your personal data.

13 This will be free to you for a trial period, and
14 then after some months you'll be converted over to a paid
15 subscription. But that's okay. You can cancel at any
16 time. In other words, we were trying to replicate the
17 kinds of product pitches that people might often
18 encounter online.

19 Then what we did is we randomly assigned our
20 research subjects -- there was about a little over 1,700
21 people in the first experiment -- and we randomly
22 assigned them to one of three conditions. And I'll show
23 you what each of these conditions look like.

24 There was a control group that really wasn't exposed
25 to any further dark patterns. There was a group that was

1 exposed to, you know, potentially a couple of dark
2 patterns, and then a group that was going to potentially
3 be exposed to a cocktail of maybe five or six different
4 dark patterns mixed together. And we wanted to see how
5 getting exposed to no dark patterns, a few dark patterns,
6 or a lot of dark patterns might affect behavior.

7 So this is what the group that didn't see any dark
8 patterns saw. They saw what I regard as a very neutral
9 choice architecture. Here's this plan. We're going to
10 go ahead and sign you up for it. But you can accept it
11 or you -- or you can decline it. There's no asymmetry
12 here. This is a simple choice between yes and no. And
13 that's unproblematic from my perspective.

14 This is what the mild dark patterns group saw. No
15 longer did they get a choice between yes and no, but
16 rather a choice between accept and continue, which is red
17 and also marked as recommended, or other options.

18 Okay. So we're seeing several dark patterns here.
19 We're making something the default choice. We're
20 suggesting that it's -- the consumers are -- would be
21 better if they went with the default. And we're also
22 putting some obstruction in front of consumers so that
23 it's going to be easier to sign up than it will be to
24 reject the data protection plan.

25 If they clicked other options, then they were going

1 to see the screen in the lower left quadrant, which is
2 some confirmshaming, a choice between I do not want to
3 protect my data or credit history, and after thinking
4 about it, I would like to go ahead and sign up for the
5 plan.

6 So if you were in the mild dark patterns condition,
7 you were exposed to these screens. One additional screen
8 that really didn't do anything significant in terms of
9 boosting our acceptance rates, but I'll show you -- as
10 I'll show you in a little bit, compared to the control
11 group, the percentage of American consumers signing up
12 for a data protection plan was very substantially higher,
13 even if they just saw these two dark patterns.

14 And then finally, as I told you earlier, there was
15 another group we called the aggressive dark patterns
16 condition, and they were potentially going to see a lot
17 of dark patterns.

18 So at first they saw the exact same screens that the
19 people in the mild dark patterns conditions saw. "Accept
20 and continue" is marked as recommended. It's checked by
21 default. And it's a choice between that and other
22 options. If they want to say no, they're going to have
23 to click through a couple of screens. If they want to
24 say yes, they're going to be able to do that really
25 easily.

1 Okay. So at the outset, the mild dark patterns and
2 the aggressive dark patterns conditions looked alike,
3 they were identical, and not surprisingly the kinds of
4 consumer responses we saw in the aggregate across these
5 two screens were quite similar.

6 But if you said no on those first couple of screens
7 and you found yourself in the aggressive dark patterns
8 condition, we were going to make you jump through some
9 additional loops in order to decline this plan that we
10 told our experimental subjects we were selling them.

11 First, you are going to have to click through up to
12 three more screens in which we shared information about
13 identity theft and why it's bad. And we wouldn't let
14 consumers advance to the next screen for ten seconds.

15 This is very similar to the kind of obstruction dark
16 pattern that Jen showed you in her slides towards the end
17 of the talk. The "while we're processing your preference
18 to not have cookies on your machine, this may take a few
19 minutes". We were basically going for a similar kind of
20 obstruction dark pattern.

21 And if they were adamant and said not "yes, I want
22 to accept", but "no, I would like to read more
23 information", they were going to have to click through
24 two more screens that looked similar to this, and then
25 finally arrive at a dark pattern that contains a very

1 confusing prompt, along the lines again of Jen's
2 examples.

3 If you select "no, cancel", are you canceling the
4 subscription or are you signing up for the subscription?
5 Well, are you sure you want to decline? No, I'm not
6 sure. Okay. There's a lot of mental energy that needs
7 to go into figuring out that if you select "no, cancel",
8 you're actually going to be accepting the plan. If you
9 want to reject the plan, you're going to have to click
10 the box that says yes.

11 Okay. So thus ended the experiment. We did want to
12 gather some more information about how people experienced
13 either the control group or the mild dark patterns or the
14 aggressive dark patterns, and so we asked people to
15 assess their moods after they finished our experiments on
16 a 1 to 7 scale. This is a standard technique in
17 psychology.

18 We asked people would you be willing to participate
19 in other research by the same researchers going forward.
20 We asked people whether they felt free to decline the
21 identity theft protection plan. And then we also had an
22 open-ended box where people were allowed to just leave us
23 comments about the experiment.

24 And then after people went through that information,
25 we explained what we were up to. We made it very clear

1 to consumers that we hadn't actually signed them up for
2 anything and wouldn't be signing them up for anything.
3 And we explained a little bit about why we were
4 interested in dark patterns.

5 Okay. So were these things effective? It turns out
6 they were highly effective. All right. So when we gave
7 people a neutral choice between yes and no, barely more
8 than 1 and 10 consumers wanted to sign up for this data
9 protection plan.

10 But if we just exposed people to a couple of dark
11 patterns, that 11 percent acceptance rate jumped all the
12 way from 25 to 26 percent. Let me -- from 11, let's say,
13 to 25.

14 Let me explain why there's three columns here.
15 Especially in the aggressive dark patterns experiment,
16 some consumers were so ticked off by our obstruction dark
17 patterns -- those three screens that you couldn't click
18 through until ten seconds had elapsed -- that they
19 actually closed out their browsers, exited the
20 experiment, and forfeited the cash that they were
21 entitled to.

22 There's an interpretive question about whether you
23 want to treat those people as having rejected the data
24 protection plan. If you do, and I think that's a
25 reasonable interpretation of the data, then the

1 acceptance rate is the third column. We call that the
2 adjusted acceptance rate.

3 If you want to exclude those people who dropped out
4 of the experiment late in the dark patterns conditions
5 from both the numerator and the denominator, then you'd
6 be focused on the middle column. There's not a big
7 difference in the mild dark patterns condition. Very few
8 people dropped off.

9 But as you can infer, in the aggressive dark
10 patterns condition, we had a pretty substantial segment
11 of our research pool, just about 5 percent of those who
12 accepted, did drop out. And so that's going to
13 meaningfully effect whether the acceptance rate is 37
14 percent or 42 percent.

15 But whether you're talking about 37 or 42, these are
16 really large numbers, right? So at the very least more
17 than tripling the acceptance rates through potentially
18 exposing people to three, four, five, or six dark
19 patterns.

20 When you think about this, these minor changes in
21 designs are very substantially boosting acceptance rates
22 in our experiment and presumably in the real world as
23 well.

24 I told you we collected a lot of demographic
25 information, and one of our hypotheses going into the

1 experiment was the dark patterns would be much more
2 successful at manipulating less educated Americans than
3 they would be at manipulating Americans with college
4 degrees or post-graduate degrees.

5 And it turns out that hypothesis was justified.
6 There were highly significant differences in the
7 vulnerability of less educated Americans versus more
8 educated Americans. And these results weren't just
9 significant, but they were very mathematically large.

10 So to give you a sense of this, in the mild dark
11 patterns condition, 21 percent of highly educated
12 Americans accepted our data protection plan, but 34
13 percent of less educated Americans accepted that plan.
14 21 percent to 34 percent, even though in the control
15 group the acceptance rates were essentially identical.

16 So these dark patterns, especially the mild dark
17 patterns, are quite successful at convincing less
18 educated Americans to accept a plan that they would
19 otherwise be inclined to reject if they were presented
20 with a neutral choice between yes and no.

21 And these results persist even when we control for
22 the fact that less educated people tend to have lower
23 incomes than highly educated people. And this is a
24 result, by the way, that we replicated in our second
25 experiment.

1 I told you as well that we collected mood
2 information from the people who we exposed to dark
3 patterns. And this is really interesting, and frankly,
4 this is one of the several results that surprised me.

5 What's interesting is that -- about this is that
6 there's no statistically significant differences between
7 those people who were exposed to no dark patterns and
8 those people who were exposed to just a couple in the
9 mild dark patterns condition.

10 They were, you know, equally happy. People in the
11 mild dark pattern condition were not statistically more
12 likely to leave us a nastygram (ph.), where we had that
13 open-ended box from comments -- for comments. They
14 weren't, you know, particularly likely to drop out of the
15 experiment. 98.5 percent of the people in the mild dark
16 patterns group continued the experiment all the way
17 through to the end.

18 That does look different when we're talking about
19 aggressive dark patterns, where people potentially saw
20 five or six dark patterns. The obstruction dark pattern
21 really did tick a lot of people off. It made them much
22 more likely to express anger. It made them -- it put
23 them in a worse mood, made them much more likely to drop
24 out of the experiment. They also said they were less
25 willing to do research with us in the future.

1 So if we try and translate our experimental results
2 to sort of what is the reality of e-commerce, what I take
3 away from our results is that there is a pretty strong
4 business incentive not to employ aggressive dark
5 patterns, not to throw dark pattern after dark pattern at
6 your customers or potential customers. That will cause,
7 I think, a lot of customers to just decide to take their
8 business elsewhere.

9 But if you just employ mild dark patterns, you just
10 employ a couple, well, that seems to be all upside.
11 There's no significant backlash from consumers, but
12 you're more than doubling the percentage of consumers who
13 are likely to accept the offer you are putting in front
14 of them.

15 And what's interesting about this mood data that I
16 showed you earlier, I said, you know, people in the
17 aggressive dark patterns condition tended to be ticked
18 off. Mathematically, this effect was entirely driven by
19 people who rejected the data protection plan.

20 People who accepted the data protection plan in the
21 mild condition or in the aggressive dark patterns
22 condition weren't actually in any worse of a mood than
23 people who accepted in the control group, i.e., people
24 who weren't exposed to any dark patterns at all.

25 Okay. So we were really intrigued by this first set

1 of results, but we wanted to go bigger. We realized that
2 there were limitations on the first study, because
3 everyone who saw dark patterns saw them in the same
4 order, saw them in the same sequence.

5 There were some really popular kinds of dark
6 patterns that we didn't test in the first experiment, so
7 we launched experiment number 2. Essentially, we doubled
8 the size of the research population. Almost 3,800
9 Americans participated in this experiment.

10 Again, this is going to be a census-weighted group,
11 so it looks just like the U.S. adult online population in
12 terms of all the relevant demographics we're likely to
13 care about.

14 And in this instance, in experiment 2, everyone was
15 only going to see mild dark patterns. They were going to
16 see one -- zero, one, two, or a maximum of three dark
17 patterns, no more than that, essentially. No one's going
18 to get an aggressive dark pattern thrown at them.

19 And the other thing we did is we randomly varied the
20 cost of the dark pattern. In the first experiment, our
21 data protection plan wasn't a terrible deal. In this
22 experiment we made -- at least for half the sample, we
23 made it a really bad deal.

24 There are commercial entities out there that charge
25 customers for data protection plans. About the most

1 expensive one that I could find on the market was 30
2 bucks a month.

3 So we randomly assigned people to either pay \$9 a
4 month or \$39 a month for this hypothetical data
5 protection plan that we told them we were signing them up
6 for. And we wanted to see, you know, how much of a
7 difference do dark patterns make compared to massive
8 price differentials.

9 And so in terms of understanding the experiment, we
10 essentially randomly assigned people to one of these 20
11 boxes. We're going to test out some dark patterns that
12 are focused on the content of the communication and some
13 that are focused on the form of the communication, and
14 then we'll be able to tell you, you know, which of the
15 dark patterns that are most and least effective and
16 whether there are any particular combinations of dark
17 patterns that are especially potent.

18 So I'll just show you a little bit about what the
19 different dark patterns looked like. In addition to the
20 control group, we had four dark patterns that were
21 focused on content.

22 One of them you can think of as a fine print dark
23 pattern. We're telling them about the free part in big
24 print. We're telling them about the cost part once the
25 pre-trial is over in smaller print that's less visually

1 prominent.

2 We're doing a social proof dark pattern. We're
3 telling them how many people just like them have signed
4 up for the data protection plan in the last couple of
5 weeks. We ran a scarcity dark pattern. You've got to
6 act now. This offer will expire in 60 seconds, so get a
7 move on.

8 And we tried a confirmshaming dark pattern, forcing
9 people, if they wanted to decline the data protection
10 plan, to say things that they're, in fact, quite unlikely
11 to believe. So those were the content dark patterns we
12 tried.

13 We also used these form-based dark patterns. The
14 control group just saw a neutral decision between
15 "accept" and "decline". But the dark patterns folks were
16 randomly assigned to boxes that might cause them to see
17 "accept" preselected by default. They could unclick
18 that, but it was going take that tiny little bit of extra
19 effort.

20 We could mark the "accept the plan" as the
21 recommended option, similar to experiment 1, or we could
22 try an obstruction dark pattern that gave them a choice
23 between "accept" and other options, which is just going
24 to make them click through one or potentially two
25 additional screens if they wanted to decline the plan,

1 but they could accept it right away.

2 And then for half of the sample, they also saw a
3 very confusing double negative prompt. Would you prefer
4 not to decline this free data protection and credit
5 history monitoring? Again, that's imposing a pretty
6 heavy cognitive demand on people, a double negative that
7 might lead people to becoming confused.

8 Okay. So what were the results of experiment 2? If
9 something is not highlighted in yellow, it's not
10 statistically significant, meaning it's not meaningfully
11 different from the control group. But if something is
12 highlighted in yellow, that means that the differences
13 we're seeing are very unlikely to be caused by random
14 chance.

15 So interestingly, that scarcity dark pattern -- if
16 you don't act within 60 seconds, this deal disappears --
17 that actually didn't increase acceptance rates. It
18 caused them to drop, though not in a statistically
19 significant way.

20 But the three other forms of content-based dark
21 patterns all significantly boosted acceptance rates. So
22 the confirmshaming strategy is boosting that acceptance
23 rate from just under 15 percent to just under 20 percent.

24 Social proof, look at how many other people have
25 signed up for this program, gets a bigger boost,

1 acceptance rate all the way up to 22.1 percent.

2 And look at what hidden information or fine print is
3 doing. All by itself, that one dark pattern is more than
4 doubling the acceptance rate. 14.8 percent becomes 30.1
5 percent just with that single dark pattern.

6 What about the form-based dark patterns? Here,
7 again, actually labeling something the recommended
8 option, to my surprise, did not significantly increase
9 the acceptance rate, but making something the default
10 choice did. And obstructing, making it harder to say no
11 than to say yes, making you click through an additional
12 screen, that caused a much bigger boost in the acceptance
13 rates.

14 And so we put these two form and content conditions
15 together, we can actually show you how these different
16 mixes of dark patterns work together, right? So we can
17 tell you that if you, you know, just do obstruction
18 alone, you're going to match up the control on the left
19 with obstruction on the top. That by itself is going to
20 boost the acceptance rate from 13.2 percent to 19.5
21 percent.

22 But look at what you can do by mixing together two
23 potent dark patterns. If you just hide the information a
24 little bit, putting it in fine print, and you make people
25 click through one additional screen, your acceptance rate

1 just from those two mild dark patterns will go from 13.2
2 percent, upper left, all the way up to 34.5 percent in
3 the -- in the lower right quadrant.

4 And so looking at this data in the aggregate can
5 tell us social scientists and some of these dark patterns
6 seem to backfire or not be especially effective, but some
7 of them can be extraordinarily effective at converting
8 people who are inclined to say no into yeses.

9 The other dark pattern that was, again, shockingly
10 potent was that double negative. So the double negative
11 question that I showed you just a little -- a little bit
12 ago all by itself doubled the acceptance rate of our
13 program from 16.7 percent all the way up to 33.4 percent.

14 And this is an instance where I think we can be
15 supremely confident that consumers are worse off. How do
16 we know that? Well, in the debrief for -- or just before
17 the debrief for experiment 2, we asked our subjects
18 whether they had accepted or rejected the data protection
19 plan.

20 And fully half of our subjects who actually accepted
21 the data protection plan on this double negative screen
22 insisted that they had rejected the plan. In other
23 words, we had bamboozled them into legally saying yes,
24 even though they understood that they were saying no.
25 And obviously with doubling, these results are going to

1 be highly significant.

2 And the other thing that was really interesting
3 about this finding, the more people -- the more time
4 people spent on the double negative screen, the worse
5 their mood and the less likely they were to do research
6 with us in the future.

7 So I'm showing you that these dark patterns really
8 matter in manipulating people who want to say no into
9 saying yes. What doesn't matter? The price doesn't
10 matter.

11 So remember, I told you we randomly varied whether
12 people were going to be charged \$9 a month or \$39 a month
13 once the one-month free trial was over. And boosting the
14 price, the monthly cost of the subscription by \$30, did
15 not significantly affect the acceptance rate. That's a
16 pretty mind-blowing result to me.

17 What are the things that really matter as consumers
18 sort of make their way through the economy and engage in
19 economic activity? We're supposed to think that price
20 drives decisions.

21 And it does to a certain extent, but here, the
22 effects of price are swamped by the manipulative effect
23 of these dark patterns. Why is that? People, as our
24 data suggests, are highly optimistic that they'll cancel
25 once the pre-trial period ends.

1 In our experiment -- experiment 2, we replicated a
2 couple other really important findings in experiment 1,
3 in addition to the ones I've already showed you.
4 People -- there was no backlash at all that showed up in
5 our data.

6 In fact, some of the dark patterns actually put
7 people in a better mood rather than a worse mood, like
8 hiding information about the price, making it less
9 visually prominent.

10 And here, again, the dark patterns were much more
11 successful at boosting acceptance rates among less
12 educated Americans than they were at boosting acceptance
13 among college graduates or people with graduate degrees.

14 So what I take away from our experiments are several
15 points. If you remember nothing about the research, I
16 would say try and remember these things. First, it's
17 mild dark patterns that are most insidious because
18 they'll substantially boost acceptance or agreement
19 without generating a meaningfully customer backlash.

20 These dark patterns do tend to prey on less educated
21 subjects. More highly educated people have built up more
22 effective defense mechanisms against dark patterns. Dark
23 patterns seem to be more important than price in
24 affecting whether people are signing up for certain kinds
25 of services or products.

1 But you don't want to talk about dark patterns with
2 a one-size-fits-all. Some of these dark patterns are
3 extremely effective. Some of them don't seem to be
4 effective at all, at least if our research is externally
5 valid.

6 And so as Jen said, these dark patterns seem to be
7 proliferating because of extensive A/B testing inside
8 firms. Before we did our research, a lot of people had
9 run experiments like this, but they had just presumably
10 kept the results proprietary. And, you know, hopefully
11 our contribution is to share those kinds of results with
12 the world.

13 So that's all I have to say as a social scientist.
14 I think I've got, like, three minutes left. So let me
15 just put on my legal scholar hat for those remaining
16 concluding remarks. And I just want to leave you with
17 sort of two points as a lawyer, as a law professor.

18 The first is that it's a mistake, I think, to view
19 the category of dark patterns as completely overlapping
20 with the category of fraud. Dark patterns and fraud are
21 both problematic, and some forms of dark patterns of
22 fraudulent, but not all of them are.

23 And second, I want to leave you with an idea about
24 how regulators might go about restricting the use of dark
25 patterns in a way that'll be comprehensible to firms,

1 transparent, in a way that doesn't give nasty surprises
2 to people who have to do the hard work of designing
3 websites or designing apps. Okay?

4 So the first point, I think, is straightforward. If
5 we think about the taxonomy of dark patterns that Jen
6 introduced at the outset, some of them are certainly
7 fraudulent, hidden information or sneaking items into
8 your cart.

9 But a lot of dark patterns are kind of in a grey
10 area involving fraud or don't involve fraud at all. It's
11 not fraudulent to obstruct someone's decision to reject
12 an offer. It's not fraudulent to nag them, to come at
13 them every two weeks until they say yes. It's not, I
14 don't think, fraudulent to employ these manipulative and
15 loaded phrases like confirmshaming.

16 And what I've done here is I've highlighted those
17 dark patterns that our results suggest are particularly
18 potent. And what you'll see is some of them are very
19 comfortably going to fit into the category of fraud, but
20 some of them really don't.

21 And so fraud should be banned. Fraud should be
22 unlawful. Fraud is bad for consumers. But there are
23 some kinds of manipulation that we see online that are
24 very hard to put into the fraudulent box but still ought
25 to be of great concern for those of us who care about

1 consumer welfare.

2 Of course, CPRA, the language that this body is
3 charged with interpreting, it doesn't include fraud as an
4 element of dark patterns. So I think it would be a
5 mistake to read into the statute something that is not
6 there.

7 And then finally, my last point is I want to
8 advocate what I'll call the symmetry principle for dark
9 patterns. If there's a grand unifying theme that
10 characterizes nearly all dark patterns, maybe all dark
11 patterns, it's a kind of asymmetry; it's a kind of
12 weighted dice or kind of stacked deck.

13 And this is, I think, an idea that both California
14 and the Federal Trade Commission have already recognized.
15 So if you look at the CCPA regulations, they build the
16 ones that are already promulgated. California has
17 already built a kind of symmetry principle into the
18 existing regulatory framework.

19 If you want to opt out of information sharing, that
20 shouldn't be harder than opting -- than opting in. The
21 Federal Trade Commission, in guidance, it recently gave
22 negative option marketing, which is like when you infer
23 from a consumer's inaction that they wish to proceed with
24 a transaction. That's what negative option marketing
25 means.

1 So too, the Federal Trade Commission had said to
2 firms, cancelation mechanisms need to be at least as easy
3 to use as the method the consumer used to initiate the
4 negative option feature. In other words, it's got to be
5 as easy to cancel as it was to sign up. It's got to be
6 as easy to say no as it is to say yes.

7 Okay. So I think that that has a really appealing
8 principle for how to regulate dark patterns. And let me
9 show you a little bit more of what I mean by that. I
10 think firms should be allowed to ask a consumer, are you
11 sure you want to say no, so long as if a consumer says
12 yes, they also see the same "are you sure" prompt.

13 I think it ought to be okay to go back to a consumer
14 who said no one month later and say "are you sure you
15 want to disable location tracking?" I think that's fine,
16 provided that that same firm also goes back to consumers
17 one month later and says to consumers who said yes, I'll
18 permit location tracking, to also reconsider their view
19 and now to opt out.

20 The problem is, dark patterns will only nag you if
21 you say no to location tracking, and if you say yes,
22 they're going to leave you alone. That's the choice that
23 the app designer wanted you to make, and so they'll stop
24 making it easy for you to change your mind.

25 So I think my view is, you want to make it hard for

1 people to say no, that's fine. Make it hard for them to
2 say yes, and there's no problematic asymmetry. There's
3 not a dark pattern, in my view.

4 And you can think about this basic approach as
5 applied to the other kinds of dark patterns that are most
6 problematic. Confirmshaming is problematic because it's
7 using manipulative language to make a seeming choice
8 between two options actually be no choice at all.

9 So think about all these valid propositions that are
10 going to be on the California ballot. Are you in favor
11 of this bond initiative to support your local public
12 schools or do you prefer that your local public schools
13 crumble and that the poor kids have to deal with, you
14 know, asbestos and falling ceiling tiles? Well, gee,
15 when you put it that way, I'll vote for the bond
16 initiative, but that's not a fair choice to present to
17 voters. And similarly, designers of user interfaces
18 ought not to be allowed to present those kinds of choices
19 to consumers and then pretend like consumers are freely
20 consenting.

21 And you know, lastly, I think this example works
22 really well for social proof. It's fine to tell people
23 that 1,647 people accepted the data protection plan, so
24 long as you tell them that 3,419 rejected it. In other
25 words, there's nothing misleading or manipulative about

1 saying three out of five dentists recommend this
2 mouthwash, but if you tell people the numerator without
3 telling them the denominator, that's more problematic.

4 And similarly -- and I think this is the last
5 symmetry principle about information that's probably the
6 trickiest to operationalize, but a dark pattern that
7 presents all the benefits of signing up for a service
8 while bearing information about the costs, it's also
9 introducing a substantial asymmetry.

10 So if consumers are likely to view the good aspects
11 of the product as material as the bad aspects or the
12 downsides or the costs, then it's easy to imagine a
13 regulatory intervention. It simply requires symmetry and
14 something that looks more like full information.

15 And so I want to be very clear about what I am and
16 what I'm not advocating here. You have to make -- as a
17 user-experience designer, you have to make hard choices.
18 Some choices are going to be really prominent, and
19 consumers will see them right away. Some of them, you
20 may you need to have people click through a number of
21 screens on settings in order to undue them.

22 The fact that it takes a few clicks to get to
23 something isn't a problem, if that thing that takes a few
24 clicks is something that very few consumers are going to
25 want to do, but if you know the stuff that consumers want

1 to do and you're putting up a whole bunch of unnecessary
2 obstacles in the path of the consumer who wants to
3 effectively exercise that choice, that's where the dark
4 pattern kicks in.

5 And so our view is, it's fine to obstruct or impede
6 or hide stuff that's really unpopular, but it's the
7 popular stuff, when you're obstructing or hiding or
8 impeding that, that you get yourselves into a lot of
9 trouble, perhaps a kind of trouble that the law ought to
10 have something to say about.

11 So if you're interested in learning more about this
12 topic or in seeing all of the underlying data that I
13 presented in the social science portion of the talk,
14 please feel free to check out the paper I did with Jamie
15 Luguri, Shing the Light on Dark Patterns. Google, Bing,
16 or any search engine will take you there.

17 And thank you so much.

18 **MS. URBAN:** Many thanks to Professor Strahilevitz
19 and Dr. King for those incredibly informative
20 presentations. We really appreciate it.

21 It's 2:08. We have two more presentations this
22 afternoon. So I'm going to call for a ten-minute break
23 so everyone can sort of shakeout a little bit and clear
24 their heads to be ready for the next presentation.

25 It is 2:08 on my clock now. So we'll reconvene at

1 2:18 p.m. for the rest of this afternoon's presentations.

2 And again, thank you very much.

3 (Whereupon, a recess was held)

4 **MS. URBAN:** Good afternoon, Mr. Gourley. I think we
5 are ready to start up again, if you want to take the
6 slide down. Thank you.

7 And are we still recording?

8 **MR. GOURLEY:** Yes. Chairperson Urban, we are ready,
9 if you're ready.

10 **MS. URBAN:** Wonderful. Perfect. Thank you so much.
11 And welcome back, everyone, from our short break to the
12 California Privacy Protection Agency's March 2022 Pre-
13 Rulemaking Informational Sessions. As you just heard us
14 discuss, we are recording.

15 We're listening to the series of presentations under
16 agenda item 2, an overview of personal information in the
17 California Consumer Privacy Act. Just to give you a
18 roadmap, we have two more presentations today, and then
19 we'll finish the day with public comment, and I'll remind
20 everybody how to engage in public comment when we get
21 there.

22 So we'll now continue with our set of informational
23 presentations. If you're following along on the agenda,
24 we're on day 1, agenda item 2, part d, Business and
25 Consumer Interactions: Communicating Business Practices

1 and Consumer Preferences.

2 I'm delighted to introduce our speaker on this
3 topic, Professor Laurie Cranor, who will be discussing
4 her work on communications between consumers and
5 businesses related to privacy.

6 Professor Lorrie Faith Cranor is the director and
7 Bosch distinguished professor of the CyLab Security and
8 Privacy Institute, and the FORE systems professor of
9 computer science and of engineering in public policy at
10 Carnegie Mellon University.

11 She is also the codirector of the Collaboratory
12 Against Hate Research and Actions Center. She directs
13 the CyLab Usable Privacy and Security Laboratory, known
14 as CUPS, and codirects the MSIT-Privacy Engineering
15 master's program.

16 In 2016, she served as chief technologist for the
17 U.S. Federal Trade Commission. She cofounded Wombat
18 Security Technologies, and she is a fellow of the ACM,
19 the IEEE, AAAS, and a member of the ACM CHI Academy -- or
20 CHI Academy, excuse me.

21 Professor Cranor, I'm delighted to turn things over
22 to you. Thank you.

23 **MS. CRANOR:** Thank you, Chairperson Urban. Let me
24 go ahead and share my slides here. Okay. Great. Okay.
25 So let me jump in here.

1 There are a few topics that I'm going to be talking
2 about today. We're going to, in general, talk about
3 different types of privacy interfaces and usability and
4 user testing that can be done with them. We're going to
5 talk about privacy policies and alternatives very
6 briefly, then, privacy icons, privacy nutrition labels
7 and tools, privacy choice interfaces, and then go over
8 some takeaways.

9 And I think, I -- you know, I listened to the last
10 set of presentations, and a lot of the things that I have
11 to say, I think resonate a lot with what you've already
12 heard today.

13 Okay. So you've all probably read a lot of privacy
14 policies, or more likely, glanced at them, and decided
15 not to read a lot of privacy policies. And people really
16 can't be blamed for not going ahead and reading privacy
17 policies because they're very long. In fact, they're so
18 long that if you were to go ahead and read all the
19 privacy policies that you encountered on websites, you
20 would likely be spending 244 hours per year in order to
21 do that. This is based on a study that I conducted with
22 Aleecia McDonald in 2008. So that's a while ago.

23 But based on what we've been seeing, things haven't
24 really gotten any better since then, and if anything, I
25 would suspect that if we recalculated the numbers today,

1 the number might even actually have gone up.

2 So we've been looking at what can we do instead of
3 having these long privacy policies, and while in some
4 sense we may need them for legal reasons, these aren't
5 necessary the best way of communicating with the public.
6 So we might, you know, somewhere on a website have the
7 privacy policy documented, but the information that we
8 want to show to people might be provided in a more user-
9 friendly way.

10 So we looked at, you know, what is the design space?
11 What are the choices of different ways that we could
12 provide privacy information to people, and there are a
13 lot of different approaches that you can take, and this
14 is kind of a, you know, a mix and match here. You can
15 play with the timing. Do you actually pop something up,
16 you know, at setup when you get a new device, when you go
17 to a new website, when you start a new program?

18 Do you instead show information just-in-time, when
19 you're prompting people to type in information, maybe
20 then, you tell them about the privacy practices just for
21 that particular information.

22 Maybe it's context-dependent, the information that
23 you provide depends on what services someone is using,
24 what part of a website they're visiting. Maybe it's
25 periodic, once a month you get a notification. Maybe

1 it's persistent like the icon that you might have in a
2 mobile app to show that location is being shared and kind
3 of sits in the corner of your screen. Or maybe this is
4 information that is only provided on demand when a user
5 specifically clicks on a link in order to access it.

6 We can also look, at you know, what channel do we
7 convey this in? If I'm using a laptop or a phone, then
8 it's likely that that information is going to be on that
9 primary channel, my screen.

10 But if I'm interacting with an IoT device, say a
11 smart light bulb or a smart thermostat, there might not
12 be a screen where we can actually provide any privacy
13 information, but generally these sorts of devices are
14 synched to another device, usually a phone, and we can
15 provide information there.

16 And then sometimes, I'm interacting with the device
17 or just passively walking by a device in a public space,
18 and so a sign on the wall might be the most appropriate
19 way to provide me with privacy information.

20 We can also think about modality. Generally, we're
21 thinking about visuals, things that we read, symbols that
22 we look at, but we can also have auditory notices, such
23 as the kinds we get when we call an 800 number, and we're
24 told, this call may be recorded, right, that's a privacy
25 notice.

1 We can have things that vibrate, and my favorite is
2 that we can have information in a machine readable format
3 which would be then conveyed to each user's device, which
4 could then convey it to the user in a way that's most
5 accessible to them.

6 We also sometimes have privacy notices that are
7 blocking. You can't move forward until you actually take
8 a look at them or at least click to acknowledge that
9 you've looked at them. Some of them are nonblocking.
10 Some of them are unrelated to your interaction with a
11 device or a website. They're just sort of sitting there
12 on the side for you to look at.

13 Here's some examples of ways that different
14 organizations have conveyed privacy information outside
15 of those long privacy policies. So you can see Apple and
16 IOS now has app privacy labels in their app store, and
17 that's kind of a shorter version of a privacy notice. It
18 uses a lot of symbols, and it distills it down to some
19 very basic facts.

20 We've seen game companies that turn their privacy
21 notice into a game. This makes it fun and intriguing.
22 I'm not sure it's the best way to actually convey
23 information, though. We've seen a lot of companies have
24 put videos on their website. Sometimes they embed them
25 in the privacy policy, and typically, these are very

1 short, like thirty seconds, to talk about a specific
2 privacy concept that's in their privacy policy.

3 And then we've had a lot of work with icons, which
4 I'm going to talk about. So let's start with icons.
5 There's been some really interesting work in designing
6 privacy icons, and there's been some great designers have
7 worked on the problems. These two icon sets that I'm
8 showing you, I think are very attractive and really nice
9 icons, but the problem with them is that unless you see
10 the words next to them, it's actually fairly difficult to
11 figure out what they mean. Most of them are not
12 particularly intuitive, and because there are so many of
13 them, it would be difficult to have people, you know,
14 learn over time what they mean. We can all learn an icon
15 or two, but you know, when you have a dozen icons, that
16 does get difficult.

17 And part of the reason why privacy icons are so
18 difficult is because privacy is kind of an amorphous
19 concept. It doesn't lend itself well to a physical
20 representation that I can draw an icon on. And so, you
21 know, the solution if you want to use icons is to put
22 words next to them, hopefully, succinct words next to
23 them, that make it more clear as to what this is showing.

24 And you may wonder, well, if you have to put words
25 next to them, why even bother with the icons? And what

1 we've seen is that there is a role for icons because the
2 icons can help attract people's attention to things. You
3 can glance at something and see the icon, and so there is
4 a role, and they can be helpful, but by themselves,
5 privacy icons are not always that useful.

6 So here's, perhaps, one of the most common privacy
7 icons that you may have seen this, trying a blue
8 triangle, I in it, which is known as the AdChoices icon,
9 and it was developed by the U.S. advertising industry.
10 And this has been deployed for over a decade now. And
11 when it first came out, we decided to do some research in
12 our lab at Carnegie Mellon to see whether people
13 recognized it, what they understood about it.

14 And we did a small study, and we discovered that
15 nobody had idea what it was, they didn't recognize it,
16 and they were afraid to actually click on it. And so we
17 did a larger study to see was it just, you know, the
18 small people -- small number of people in Pittsburgh who
19 came to our lab, or was this a bigger problem?

20 So we did this online using the crowdsourcing
21 service, Amazon Mechanical Turk, and we had over 1,500
22 participants, and we showed these participants this icon,
23 and we varied the tagline. So usually, when you see it,
24 either there are no words next to it, or you have the
25 words, AdChoices, but sometimes, you see other taglines,

1 such as, "Why did I get this ad?" And so we wanted to
2 see whether people understood it without a tagline and
3 whether the different taglines would make a difference.

4 So we showed people an ad with the icon and a
5 tagline or not, and then we asked them questions, like
6 what would happen if you clicked on the icon? And then,
7 we gave them a number of choices, and they could tell us
8 likely they thought it was that each of these things
9 might happen.

10 So more than half the people told us that it was
11 likely that more ads would pop up, and that's incorrect.
12 That will not happen if you click on the AdChoices icon.
13 Almost half the people thought it was kind of a, your
14 ad's here, sort of thing, if you want to buy an ad, you
15 should click on the icon, and that's also incorrect.

16 So only 27 percent of people had the correct answer,
17 which is that this will take you to a page where you can
18 opt out of tailored ads. So that was the results we
19 found when we put the word, AdChoices, next to this icon.

20 However, as I mentioned, we tried a bunch of other
21 taglines, and the one that we found was most successful
22 was "Configure ad preferences." When we showed,
23 "Configure ad preferences," actually 50 percent of the
24 people realized the correct answer.

25 Now, you can see we still had a lot of

1 misconceptions. So this is not a perfect solution, but
2 it is by far better than the solution of putting
3 AdChoices next to it. And we published these results a
4 decade ago. Nonetheless, we still see that usually
5 AdChoices is the term that is next to it, and this is
6 also from an industry that does a lot of A/B testing and
7 could probably come up with something even better than
8 what we came up with.

9 All right. So the next icon that I want to talk
10 about is the icon for the CCPA. So when the CCPA
11 legislation came out, my students in my lab at Carnegie
12 Mellon -- even though we're in Pittsburgh, we're not in
13 California, but we read it, and we noticed that there was
14 a provision to have a button or a logo that would sit
15 next to the, "Do not sell my personal information link."
16 So we were curious about that and found out that there
17 had been nothing proposed, and so we decided to try to
18 come up with something ourselves within the ninety-day
19 public comment period.

20 So we didn't just want to come up with an icon,
21 though. We wanted to actually test it and find out if it
22 was any good before we proposed it to the attorney
23 general. So there was a lot of work to do, but my
24 students are great, and we did actually do all of this
25 within ninety days. So we came up with icons. We did a

1 preliminary evaluation. We refined the most promising
2 icons. We tested the refined icons. Then, because we
3 knew from past experience how important the text was, and
4 we weren't so sure that the text that's in the
5 legislation was the best, we decided to test some other
6 text.

7 And then we combined the icons and the text, and we
8 submitted our comments during the ninety-day public
9 comment period. We, later, actually collected some more
10 data and wrote a paper about it which is also published,
11 and it's on our website.

12 Okay. So this was the ideation phase. We actually
13 had some workshops at Carnegie Mellon and with our
14 collaborators at the University of Michigan where we
15 asked people to think about what -- how would you convey,
16 "Do not sell my personal information"? What visuals come
17 to mind. And people sat there with stacks of Post-it
18 Notes and markers and came up with ideas. These weren't
19 designers or artists. These were just everyday people
20 and a lot of people who thought a lot about privacy
21 coming up with ideas.

22 And there were three general concepts that we
23 noticed when we put them all on the whiteboard and
24 rearranged and said, you know, what do we have in common?
25 So we had some people who tried to draw a picture that

1 represented choices and consent, other people tried to
2 represent the concept of opting out, and then we had
3 people who tried to represent the concept of not selling.
4 Those were -- I mean, there were a few others as well,
5 but these were the main concepts that we saw.

6 So we took these ideas and our badly drawing Post-it
7 Notes, and we gave them to some designers and had them
8 try to actually polish these and make them look nice. So
9 here are our three favorites related to choice and
10 consent. Here we have opting out. You'll notice the
11 idea with opting out is that we have a box, a hole, and a
12 folder, and we have the arrow showing that you're lifting
13 something out of them. At least, that was the plan of
14 what we were trying to convey.

15 And then we had the icons that represented, do not
16 sell, and so you can see we have dollar signs
17 representing selling and then different ways of not
18 selling, with a slash, or a do not enter, or a stop sign
19 as well with that.

20 We also noticed that the advertising industry had
21 put forward a green version of their blue icon, and they
22 claimed that that would represent, "Do not sell my
23 personal information." So we decided that we might as
24 well test that as well.

25 Okay. So for our first evaluation, we did this

1 again, on Amazon Mechanical Turk. This was a relatively
2 small study with 240 participants. And we tested our
3 twelve icons, both with and without the tagline, "Do not
4 sell my personal information." So half the people saw
5 that, half of them did not.

6 Each person saw one icon, and we asked them what
7 they thought the icon meant and what they thought would
8 happen if you click on it. Then, we showed them the
9 whole set of twelve icons, and we asked them, which one
10 do you think best conveys the idea of "Do not sell my
11 personal information," and which one best conveys the
12 idea of privacy choices?

13 So here's what we found, first of all, we found that
14 without the words, people had a lot of trouble figuring
15 out what any of these icons meant. So the words -- as
16 we'd seen earlier, the words were actually pretty
17 important.

18 We found that this icon that looks sort of like a
19 stylized toggle is what best conveyed the idea of choices
20 about personal information. And this icon with a dollar
21 sign and a slash was what best conveyed the idea of "Do
22 not sell my personal information."

23 But we also found very strongly that people thought
24 it had something to do with payments or no payments or no
25 cash or no money or something like that. So it also had

1 a lot of misconceptions associated with it.

2 These opt-out icons were mostly confusing to most
3 people. They did not understand what we were trying to
4 convey there. We found that very few people recognized
5 that this black octagon with a dollar sign was supposed
6 to represent a stop sign. Maybe it was because it was
7 because it was black and not red. I don't know. But in
8 any case, it didn't really work very well. And we also
9 found that people had really no clue about this green
10 triangle.

11 So we decided to take the two that seemed the most
12 promising and refine them. We were also curious whether
13 if we made the stop sign red, whether that would actually
14 help. So we decided to make it red and try that, and we
15 also brought the green triangle along as well, and so we
16 now had these colorized versions of these icons with some
17 tweaks to them, and we did another evaluation.

18 And so we did a similar study, and once again, we
19 found that the dollar sign with the slash best conveyed,
20 "Do not sell my personal information." Didn't do a very
21 good job of conveying the idea of choices. And we found
22 that the stylized toggle did a good job of conveying
23 choices, but didn't do as good a job with "Do not sell my
24 personal information." And the other icons were not as
25 good at anything.

1 We also looked at the common interpretations of each
2 of the icons. Here were some of the most common things
3 that we saw. With the toggle, we saw a lot of correct
4 interpretations. Now, they didn't address privacy
5 specifically, but they did understand that it was related
6 to activating, declining, deactivating, those sorts of
7 things.

8 The slash dollar, unfortunately, we just saw a lot
9 of associations with money, things being free, and we
10 only saw one person who understood that it meant selling
11 is not allowed. Again, none of these conveyed privacy
12 specifically in this case.

13 The green triangle, a lot of people thought it had
14 to do with getting more information or that it was a play
15 button for an audio or video player.

16 All right. Then we did some ideation on taglines.
17 So besides the "Do not sell my personal information" and
18 "Do not sell my info," which are in the regulation, we
19 also tested a bunch of other things that we thought had
20 potential to be better for consumers. And the top ones
21 from our testing were "privacy choices, privacy options,"
22 and "personal info choices."

23 So then we did combo testing. So we tested three
24 icons and five taglines, plus no tagline. We also tested
25 no icon. So we had 4 icon conditions, 6 tagline

1 conditions, 4 times 6 is 24. We did not test having no
2 icon and no tagline because that would convey nothing.
3 So we did twenty-three different conditions in our test.

4 And the way we tested them, again, this was on
5 Mechanical Turk, but we wanted to put this in the context
6 of a website. So we made up a footwear website, and it
7 looked like a typical e-commerce website, and it had lots
8 of, you know, information on the bottom of the screen,
9 privacy policies and shipping policies and things like
10 that, and we put at the bottom an icon and a tagline.

11 And in our study, each participant saw one of these
12 conditions, so 1 of the 23 conditions indicated what
13 combination they would see there. So we showed them that
14 website, and then we gave them a survey where we gave
15 them a close-up so that they could make sure to see what
16 this was, and we asked them, what do you think would
17 happen if you clicked on this?

18 So once again, we saw a lot of misconceptions, and
19 because we had this in the context of a website this
20 time, a lot of the misconceptions had to do with the
21 website. So they thought that personal info had to do
22 with shoe sizes, for example, and payment methods on the
23 website.

24 We also saw that the slash dollar sometimes suggest
25 to people things related to payment options or encrypted

1 payments. We saw that the toggle icon usually didn't
2 have misconceptions, but there were a small number of
3 people who thought maybe it was a real toggle, not just a
4 symbol related to being a stylized toggle.

5 We found that none of the icons were very good
6 without a tagline, once again, and the slash dollar was
7 especially bad when we didn't have a tagline.

8 We also found that if we had the taglines without
9 the icons, it was fine. They didn't really have -- the
10 icons didn't really have that much impact on the
11 interpretation of the taglines.

12 So based on this study, we wrote our report, and we
13 recommended this blue stylized toggle icon, and we
14 recommended putting the tagline "Privacy options" next to
15 it. The idea here being that this would allow consumers
16 to look for one button for all their privacy-related
17 choices, right, we don't really want to have different
18 privacy regulations for different specific things, both
19 in California and around the world where, you know, each
20 regulation has a different icon, and you'd have, like,
21 all these different icons. You'd have to click here for
22 the California opt-out and here for the Texas opt-out and
23 here for Europe, and that really didn't make much sense,
24 and we thought well, if we could just have one icon, we
25 could click, and you'd get all your choices, that would

1 simplify things.

2 Now, that said, that's not what is actually in the
3 legislation, and so of course, you could also put this
4 next to "Do not sell my personal information."

5 Okay. So this is what we recommended, and this is
6 what the Office of the Attorney General put out for
7 public comment shortly after we submitted our
8 recommendations. And at first, we looked at it, and we
9 said, okay. They have an icon that is also kind of a
10 stylized toggle, like what we suggested. We suggested
11 blue, they suggested red, but you know, it's kind of
12 similar. But then we started to think about it, and we
13 had some concerns.

14 We had specifically designed our stylized toggle not
15 to look like a real toggle to try to prevent the case
16 where people would think that they should toggle it. And
17 by making it blue, we also tried to prevent people from
18 trying to infer what state it was in. So seeing
19 something red and something that looks a lot like a
20 typical toggle that people see in IOS or on a website
21 made us concern that people would try to toggle it and
22 that people would view the red coloring as inferring some
23 sort of a state.

24 And there were other people who were concerned about
25 this as well. We saw a lot of tweets on Twitter where

1 people were complaining that they thought that this would
2 be fairly confusing.

3 So we decided to run another study and test what we
4 had proposed against this new red icon. While we were at
5 it, we made another version of it that had a bigger X.
6 We thought it was more aesthetically pleasing, and then
7 we decided, well, let's test ours in red and the other
8 one in blue as well. So we tested, you know, six
9 different versions of this.

10 We found that the size of the X made very little
11 difference, but we did find that there was a big
12 difference between what we had proposed and the red icon
13 that had been proposed. We found that the red one was
14 much more likely to be misinterpreted as an actual
15 toggle, and therefore, people said that they might not
16 click on it because they were afraid of changing the
17 state of things into something bad. We found small
18 differences based on color. That turned out not to be
19 that big a deal in this case.

20 So a big takeaway, though, was that it was really
21 important to do this test. I think, you know, what had
22 been proposed by the Attorney General's Office seemed, at
23 first, to be a relatively small changes, but they
24 actually made some big differences. And so it was
25 important to actually do the user study to find out what

1 the impact would be.

2 So as a result, the Attorney General's Office
3 removed the icon from the regulation and said they would
4 come back to it later.

5 And we went ahead and tested some more icons. So we
6 tested some variations on the ones we tested before and
7 some others that had been suggested to us. And this
8 time, we made some changes to our study. So we also
9 looked at whether any of the icons would help in
10 communicating, "Do not sell," choices, whether it would
11 help in standing out to users on a website, and whether
12 they would help motivate users to actually click, which
13 is, you know, what we want people to do. If they
14 actually want to opt out, they're going to need to click
15 on something.

16 And this time, we also made sure that all of our
17 participants were California residents. They were not
18 from people all over the U.S., since it's most relevant
19 to California residents.

20 So what did we found out? We found out that we
21 could communicate best if we had no icon. So that was
22 kind of disappointing. We also found that adding any
23 icon, the good thing about it, is that it made users more
24 likely to notice the link. So it did help with standing
25 out on the website, but it didn't create a significantly

1 higher motivation to click on the link.

2 So having any of these particular icons was hurting
3 communication, but it was attracting attention. So this
4 suggests to us that there's still some hope for icons,
5 that having an icon can help you attract attention, but
6 we need one that doesn't convey the wrong information.
7 And so perhaps, we should revisit that icon that we
8 tested earlier which seemed to have fewer misconceptions
9 associated with it.

10 And in fact, that's eventually what the Attorney
11 General's Office did, and they recommended our icon. So
12 we were very excited. Our icon is now the CCPA Privacy
13 Options icon. However, you know, it's been a year or so,
14 and well, it hasn't really been adopted. I had been
15 looking for it, and I see it on my website. That's about
16 it.

17 So there's a question that if we want this icon or
18 any icon to be adopted if it is a voluntary icon, how do
19 we actually adoption because it seems that companies are
20 not, just you know, on their own, deciding that they want
21 to adopt it?

22 Okay. Let's talk about privacy nutrition labels and
23 tools now. So there's been a lot of discussion for
24 probably about twenty years now where people have said,
25 hey, we don't want to read these long privacy policies.

1 Let's just make it so easy like reading a nutrition label
2 on a food wrapper where you can just glance at it and get
3 information.

4 So in about -- I think we started working on this
5 about 2007, 2008. My students started trying to figure
6 out what that sort of design would look like for a
7 privacy nutrition label. And we did focus groups; we did
8 online testing; we did lab testing, and this is a design
9 that we came up with that tested well in our studies.
10 And you can read the papers about it, if you want. This
11 hasn't actually been adopted. Another no-adoption.

12 But what we learned from this is that what's really
13 important here is that it's succinct and it's
14 standardized. So you know, if every company comes up
15 with their own nutrition label, that's not very useful.
16 What we need is them all to follow the same template, so
17 you can put them side by side, and you can compare them,
18 and this makes it much easier for users to figure out
19 what kinds of data is being collected and what is going
20 to be done with it.

21 Okay. We also looked at, could you do something
22 even smaller than a label, some sort of like privacy
23 meter, and if you had privacy meters, would people pay
24 attention to them? Would they actually be attracted to
25 websites that have better privacy according to a privacy

1 meter?

2 So we developed a privacy meter for a search engine,
3 and we did a study where we had people come into our lab,
4 and some people were shown a search engine with no
5 privacy meters. It also had a price comparison. So you
6 can see on the right side, we have the prices with
7 shipping for all those items, and on the left side, we
8 have the privacy meter.

9 So some people saw this search engine without the
10 privacy meter, just the prices, and you know, the prices
11 influenced their decisions, and some people saw it with
12 the privacy meter. We also had some other variations
13 that we use as control conditions here.

14 But what we found was that when we did not show
15 people a privacy meter, they would typically go for the
16 cheapest site to make their purchases. And in this
17 study, people actually did use their credit cards and
18 actually made purchases.

19 But when we showed them the privacy meter, then we
20 found that people were often influenced to pay a little
21 bit more to shop at the website with better privacy.

22 We also tried some variations on this where we put
23 the privacy meter in the header of a website or in an
24 interfacial page. So you click on a link, you see the
25 privacy meter, and then you click through to the website.

1 And we found that if we took the privacy meter out
2 of the search engine and put it somewhere else that the
3 effect went away. So it was most useful when it was
4 right there when they were making the decision in the
5 search engine about where they should click.

6 Here's an example of one of the ways we tried that
7 was not effective where we put it at the top of the page.

8 So we've also looked at bank privacy policies, and
9 bank privacy policies were actually standardized through
10 a collaboration of a whole bunch of U.S. federal agencies
11 who regulate the U.S. financial sector. This was done
12 about a decade ago. And so every U.S. bank you go to
13 now, pretty much, they have their privacy policy in a
14 format that looks like this. The colors vary, the fonts
15 vary, but it's basically this sort of a format, and you
16 can actually put them side by side and compare them.

17 One problem, though, is you go into a bank and you
18 look at their policy, or you go to their website, you
19 look at their policy, and if you don't like it, then how
20 do you find a bank that has a policy that you do like?
21 This becomes a very long and iterative process.

22 So what we decided to do was to crawl the web, find
23 these policies, screen scrape them all, put them in a big
24 database, and make it searchable. So now, you can type
25 in your zip code and find banks near you and compare

1 their privacy policies very easily.

2 We did this as a prototype. We're not actually
3 maintaining this as a service. So you can try it on our
4 website, but it's not up to date at this point, but it's
5 a proof of concept. And this basically demonstrates the
6 power of once you have standardized information, this
7 allows you to make useful tools for users, even better if
8 the standardized information is in a computer-readable
9 format so that it makes it very easy to build these
10 tools.

11 All right. Here's another privacy nutrition label.
12 This one's actually for privacy and security. This is a
13 project we did at Carnegie Mellon to develop a label for
14 IoT devices. The idea is this would be on the packaging
15 of an IoT device or on a website that's selling IoT
16 devices. And we did some studies with experts to find
17 out what information we should put on them, and experts
18 had a lot of information, especially about security, that
19 they thought should be on these labels.

20 So what we did is we took what we thought was most
21 important for consumers, we put it in the version that's
22 on the left. That's the nice, succinct version, and then
23 we put a link and a QR code that you could scan to get
24 the detailed version for experts.

25 And what we found in our user studies is that this

1 is actually very helpful to consumers, and we tested to
2 see, like can consumers handle this? Can they understand
3 this information? And we found for the most part that
4 consumers did have an idea of which devices would be more
5 or less risky for them to purchase and deploy in their
6 homes based on the information. And you know, we found
7 some things that were less clear to consumers, and we've
8 gone ahead and worked on trying to reword to make it
9 better for consumers.

10 Then, once we had that label, again, we had the
11 question of all right. So the consumer finds their, you
12 know, smart thermostat or smart doorbell, and it's not
13 good on privacy or security, how do they find a better
14 one, and how can they do this comparison shopping?

15 So this is a prototype of an app that you could run
16 on your phone which would let you do the comparisons, but
17 in this case, there's a lot of information, and so we set
18 this up so that consumers can indicate which aspects they
19 care most about, that's their priority settings. They
20 can set their preferences for what is acceptable for each
21 of the priority settings, and then they get a device
22 comparison where here you see two devices side by side,
23 and it lights up in red which ones don't match their
24 preferences, and in white, those that do. And so you can
25 more easily compare these devices without having to try

1 to like put these policies all side by side on your small
2 computer screen or on your phone screen, which would be
3 impossible. If you took this and then integrated it with
4 a search engine, you'd have something even more useful.

5 Here's a project that we did about ten years ago to
6 develop an app nutrition label for the Android App Store.
7 We developed this privacy facts, and we wanted to test it
8 with consumers to see whether it would actually help
9 people choose apps and consider privacy.

10 And so here, we came up with the idea of inviting
11 people to our lab and asking them to help a friend who
12 has a new smartphone choose some apps, and we gave them a
13 list of the types of apps that their friend wanted, a
14 word game, a diet app, a travel app, things like that.
15 And then, we gave them our mocked up version of the app
16 store where they could choose from two of each type of
17 app that their friend was interested in.

18 Half the people saw our app store with privacy
19 facts, and half of them saw it without privacy facts.
20 And what we found is that those who saw the app store
21 without privacy facts had all sorts of reasons for their
22 selections, but none of them had anything to do with
23 privacy. But those who saw privacy facts were much more
24 likely to say, oh, I chose this one because it's better
25 for privacy, but privacy wasn't everything.

1 We saw cases where they actually did not choose the
2 more privacy-protective one, and those were generally
3 cases where they said, hey, I've used this app; I know
4 this brand; I think it's great, or look, this one has five
5 stars, the more privacy-protective one only has two
6 stars; I'm going to go with the five stars. So privacy
7 is not everything, but when you have that information, we
8 found that people were actually able to use it.

9 So as I mentioned, this is research we did about a
10 decade ago. Fast-forward ten years, finally, Apple comes
11 out with an app privacy nutrition label for the IOS
12 Store, and Android is supposed to be coming out with
13 something similar next month.

14 So we were really excited to see this actually
15 deployed and have started doing some research to see, is
16 this actually useful? Our initial studies with IOS
17 suggests that there's a lot of confusing terminology in
18 what has been deployed, unfortunately, a lot of confusing
19 definitions.

20 And so we've done studies with app developers, and
21 found that the app developers are having trouble filling
22 this out accurately, which means that some of these
23 labels probably are wrong. They're not actually
24 reflecting what's going on because the developers don't
25 understand how to fill them out. And we have a paper on

1 that that is coming out, and we already have it on our
2 website.

3 We also did a study with consumers, which we're
4 still writing up, and with consumers we also saw similar
5 things, where consumers were confused by some of the
6 terminology. We haven't yet delved into the Android
7 version yet.

8 But basically, you know, the big takeaway here is I
9 think privacy nutrition labels for apps are still a great
10 idea, but I think they do need some extensive testing,
11 both with users and developers, to make sure we have
12 something that it's going to be understandable and
13 usable.

14 Okay. Let's take a look at privacy choice
15 interfaces. So these are everywhere, and we, in the
16 previous presentations today, have already heard about
17 some of them. These include cookie banners, audience
18 controls on social media, the app permissions, third-
19 party advertising controls, marketing opt-outs, and then
20 of course, CCPA and GDPR rights interfaces.

21 So what makes these interfaces useable? So we've
22 done some work to try to identify some specific usability
23 features that we might want to look for and evaluate for.
24 And so here's our list: first of all, it should meet
25 users' needs. It should actually give people the choices

1 that they want. It should require minimal user effort.
2 It should make users of the fact that choices actually
3 exists and where to find them. It should be
4 comprehensible to convey choices and their implications
5 so that users understand them. It should do all of this
6 in a way that the users are satisfied with the interface,
7 and they trust it. It should be done in a way that users
8 can change their mind, and if they make a mistake that
9 they can fix their errors. And it shouldn't nudge users
10 towards the less privacy-protective options. It
11 shouldn't have dark patterns.

12 Okay. So we've seen lots of bad interfaces, and in
13 the previous presentations, there were lots of examples
14 of this. You know, here's an example similar to what
15 you've already seen this afternoon of a toggle that it's
16 not quite clear what state the toggle is in and what
17 would happen if you toggled it the other way.

18 We've also seen in our research that, you know, many
19 of these interfaces, if you want to find this toggle, you
20 have to scroll, scroll, scroll, scroll, scroll all the
21 way to the bottom of the screen, and find a little tiny
22 link. They're not at the top of the screen. They're not
23 floating where you would find them. And we find that
24 they're all different. They're not standardized. You
25 learn how to use one, that doesn't mean you're going to

1 be able to use another one.

2 And even when they use a standardized platform --
3 because there are a small number of companies that
4 actually sell the interface components to websites they
5 can use so that they can, you know, just deploy these
6 choice without having to code it up themselves. So you
7 would think this is, like, fairly standardized, but we've
8 seen is that the standardized platforms offer many
9 choices, lots of flexibility to websites, and so the end
10 result is that they all do things differently, and we
11 don't actually have that standardization for users.

12 Okay. So my colleague Eleanor Birrell at Pomona and
13 her students have done some user studies testing several
14 CCPA opt-out user interface variations. They have a
15 paper on this that you should check out. And basically,
16 what they found, not surprisingly, you know, based on
17 what we've seen in other research is that how you design
18 this interface makes a huge difference on opt-out rates.

19 If you just give people one big "Do not sell my
20 information" button, you get many more people clicking
21 it, then if you give people multiple buttons or if you
22 give people a button and a link, and you know, they have
23 to, if they want a do not sell, then they have to go and
24 click on the link. And so all of these things make a
25 difference.

1 One of the things that Eleanor Birrell and her
2 students did to try to make this better for users was to
3 say, well, what if you didn't have to go look for that
4 link in the bottom of the page and figure out what it
5 means? And so they developed a plugin, which is
6 available as a Chrome extension -- and you can search for
7 it in the Chrome Web Store -- that will automatically
8 find that link for you on the page and make this little
9 widget, and you don't have to scroll down. It's just
10 going to sit in the corner of your screen, and there's
11 one button there, "Do not sell my personal information,"
12 all you have to do is click it. And so that's an
13 interesting kind of standardized approach where, all
14 right. The websites aren't going to be standardized.
15 Okay. Well, we'll put something on top of that that
16 makes it standard with this widget. You can also imagine
17 that a browser company could even build that into their
18 browser.

19 Speaking of building into the browser, another
20 approach is global privacy control. Again, the idea is
21 to let your browser be your privacy agent. You can set
22 once what your preference is about opting out, and your
23 browser could then send that signal to websites.

24 We don't have universal adoption of this, like we
25 don't have a lot of adoption of this yet, but this is

1 something that hopefully going forward, we'll have
2 another easy way for users to access this. Also, think
3 it's important because users may not know whether or not
4 a website respects their opt-out signal is to have some
5 sort of an indicator in the browser to indicate, yes.
6 This website has accepted your opt-out signal or this one
7 has not.

8 Another tool that was developed by my colleagues at
9 Carnegie Mellon was a tool that would look for all kinds
10 of opt outs, not just CCPA, on websites. And again, this
11 the browser plug-in. And it finds all the opt outs for
12 you, and then you can go through and choose which ones
13 you would like to opt out. This is called Opt-Out Easy.

14 Okay. Let's take a look at cookie banners, and we've
15 already heard us some of this and a little short on time.
16 So I'm going go through some of this quickly. There are
17 a lot of problems with common cookie banners that we see.
18 They have defaults which are not privacy protective.
19 That they in fact often default to the least privacy
20 protective option, and in our fairly confusing. They
21 require you to check multiple places to know what your
22 confirming. You know, this example here we can confirm
23 my choices, but I only actually see on the screen one of
24 the choices that I'm confirming. And I would have to
25 actually go through four different tabs before I knew

1 what I was actually confirming.

2 Sometimes they have no choices, which is kind of
3 pointless. Sometimes they do that confirm shaming thing
4 we talked about. You know, this is an example of an
5 organic food store, and you know they're are kind of
6 misleading you in a way by talking about you know, the
7 quality of the organic ingredients. Oh wait, what that
8 have to do with these cookies, you know, their -- it may
9 be that their -- the cookies they sell in their store are
10 organic but that doesn't make any sense when we talk
11 about web cookies.

12 We see that even when you use the consent management
13 platforms that we have this problem. So here are two
14 banners that we generated ourselves. We used one of the
15 consent management platforms and we generated this with
16 the platform. And the platform is happy to allow you to
17 generate either approach for your website. The one in
18 the top, we have a button that says accept all cookies,
19 and its bold and there's a link to edit cookie
20 preferences. And if you click the link then you have to
21 go through more clicks and links in order to get the
22 preferences that you want.

23 A better approach, I think, is that you put the
24 choices right there on the screen. So we have except all
25 cookies, but just as easy is I can accept only necessary

1 cookies. And if I'd like to do something more fine-
2 grained, then I can click edit cookie preferences and go
3 decide exactly which cookies that I want. And so -- you
4 know, ideally, we would have some nudging of web
5 developers to say do this one, don't do the one with just
6 the link. Even though the cookie management platforms
7 make that really easy to do.

8 All right. I am going to tell you little bit about
9 a study that we did evaluating different cookie banners
10 and that the impact of them was. So we started by taking
11 a look at about 200 websites and looking to see what were
12 the popular things that were being done. And then we
13 developed 12 different variations of the same cookie
14 consent banner.

15 And I'm going to skip over this, and right here is
16 our website. We designed website called Cups and Such.
17 It sells cups and drinkware. And we invited people to
18 come test out this website, and we asked them to find
19 some cups they were interested in buying and put them in
20 their cart and then we would give them a survey. And in
21 the survey we them some questions about the cookie
22 consent that oh, by the way, that popped up while they
23 were on the website. Then we have them go back and look
24 at it more carefully and answer some more questions.

25 We had over a thousand participants in the study.

1 Unfortunately, it turned out that most of them were young
2 women. We did not have a very diverse sample in this
3 case and were actually working on doing the study again
4 to test a bunch of things, but in part to have a more
5 diverse sample.

6 Okay. So this was one of the variations that we
7 tested. And this is -- we called it best practices. You
8 could probably do better, but this was the best of the
9 ones that we tested. This has a fully blocking design,
10 so you have to interact with it. It doesn't just sit in
11 the corner. It shows you in line all of the cookie
12 options right there. You don't have to click through.
13 It has bulleted text rather than the big paragraph. And
14 it has detailed button text, so it doesn't just say,
15 like, okay. It says allow all cookies, allow selected
16 cookies. And if you click show details then you get not
17 multiple tabs, but a single layer with all the detailed
18 definitions of each type of cookie. And it even explains
19 what you should do if you change your mind, and it has a
20 cookie preferences button, which you can see in the
21 bottom right, which always sits on the screen on the
22 website. So you can so you can always come back and
23 reverse your decision.

24 Then we had a worse practices variant that did a lot
25 of things wrong. This -- the banner design at the bottom

1 of the page. You can ignore it. You don't have to
2 interact with it. It has - it has a link; not a button,
3 if you want to go and change your preferences. And we
4 had this interface with all these different tabs rather
5 than everything on all on one page. It even has some
6 texts that suggest to you that you might be losing out if
7 you don't accept all the cookies. It's a big paragraph
8 of text, and we have just a generic okay button. It's
9 not entirely sure what that does. It doesn't mention any
10 way of reversing your decision if you change your mind.
11 Okay. And this is what it looks like on a website.

12 Okay. Then we had a variant where we didn't have
13 any banner. We just had a cookie preferences button that
14 would then show you this cookie preferences screen. And
15 so it looked like this. You come to the website and you
16 could easily ignore it if you wanted to. I don't have
17 time to go through all the different variations, but we
18 tested a bunch of other things so that we could isolate,
19 you know, whether there was a banner at the bottom the
20 screen, or whether is the center of the screen. Whether
21 there was a link or whether it's a button. Whether we
22 had bullets or paragraphs. So lots of different
23 variations and we isolated each one of them.

24 And here's what our results are. So each of these
25 horizontal bars represents a condition. And what we're

1 seeing here is the percentage of participants who made
2 each decision. So the red participants, they were the
3 ones who said I only want strictly necessary cookies.
4 The blue ones, not very many, made some very specific
5 decision of allowing some cookies but not others. The
6 green ones took all cookies, and the purple ones didn't
7 make any choice at all when they were on the website.

8 And what we can see is that for the best practices
9 and some of the small changes that we made, we have a lot
10 of participants who said hey, I'm not going to take all
11 cookies. I just want strictly necessary. But in the
12 conditions where they weren't shown all the options, most
13 people just took all cookies, or even worse in the
14 nonblocking ones where they could ignore it, well, a lot
15 of them did. And they just didn't interact with it at
16 all.

17 Okay. So we see that the absence of a fully
18 blocking or banner notice led to poor awareness. You
19 know, if you just put that cookie preferences in the
20 corner and do nothing else, and there are real websites
21 to do this, most people completely ignore it. And in
22 fact, most of them don't even notice that it's there. We
23 also find that if we don't show people the options, they
24 have a lot less investment in their decision-making. We
25 found that after people made their decision, if there was

1 a cookie preferences button, then they were much more
2 able to figure out how to reverse their decision later.
3 Even though in all cases there was a cookie preferences
4 link buried in the bottom, but we had many more people
5 who said that they understood how to reverse their
6 preference when it was a button versus when it was a
7 link.

8 And we found that the names of the cookie categories
9 themselves, performance cookies and functional cookies,
10 which are the standard that has been used for a long
11 time, completely confused people. Only 16 percent of
12 participants understood what functional cookies were.
13 And so this seems pretty problematic and maybe we should
14 come up with better terminology.

15 Okay. And then finally, I want to mention this
16 notion of the burden of user consent. Doing all this on
17 every website is a lot of burden for users. And we
18 really should think about solutions that don't require
19 users to jump through all these hoops and do all this on
20 every website.

21 So finally some takeaways here. So first of all,
22 there -- we should be thinking about alternatives to long
23 privacy notices that can help users obtain information
24 they need quickly. Icons might be a good idea, but we
25 have to remember that it's difficult to convey privacy

1 concept with icons, and we should think about having
2 accompanying words when we have icons. We should try to
3 reduce the user burden by having standardized interfaces,
4 search engines, and user agents, so that users don't have
5 to go read all this at every website they visit with
6 every device that they use. We should incentivize the
7 adoption of the privacy options button and other
8 standardized interfaces. We should remember that
9 interface design has a large impact on the choices people
10 make, and the previous speaker showed you that. I showed
11 you more data about that, and we really need to make in
12 the context of cookies accept only necessary cookies
13 should be just as easy as accept all cookies.

14 And then whatever you do, do user testing. User
15 testing is essential for evaluating usability. You can't
16 just look at it and say oh yeah, I know what users are
17 going to do here. And there are a bunch of different
18 things that we should probably consider when we do user
19 testing and we've outlined them here.

20 All right. So that's it for me for today. Thank
21 you.

22 **MS. URBAN:** Thank you very much, Professor Cranor.
23 Much appreciated. A very, very informative presentation.

24 So I'll just wait for -- wonderful -- for the slides
25

1 not to be shown anymore. And I'm now pleased to
2 introduce our final speaker for today, Ms. Stacey
3 Schesser, who will be discussing opt out preference
4 signals in the California Consumer Privacy Act.

5

6 Stacey Schesser is the supervising Deputy Attorney
7 General for the privacy unit in the consumer protection
8 section of the Office of the California Attorney General.
9 Her recent matters include People v. Glow, People v.
10 Equifax, and leading the team that drafted regulations
11 for the California Consumer Privacy Act. As contemplated
12 in the California Privacy Rights Act of 2020, Ms.
13 Schesser is supporting the CCPA in its work. Ms.

14 Ms. Schesser began her career at the Attorney
15 General's Office in 2007 in its criminal division and has
16 worked in the privacy unit since that unit's inception
17 in 2012. In 2019, Ms. Schesser was recognized as one of
18 the recorders Women Leaders in Tech Law, and she was the
19 only public-sector recipient of this award.

20 Ms. Schesser received her JD at the University of
21 California because Berkeley School of Law, where she
22 wrote on privacy issues for the California Law Review.
23 She received her BA at Douglas College in Rutgers
24 University.

25 Ms. Schesser, welcome and the floor is yours.

1 **MS. SCHESSER:** Thank you so much. I'm going to
2 share my screen to begin my presentation.

3 Okay. Good afternoon and thank you so much for
4 having me. I am going to be presenting on opt out
5 preference signals and the CCPA. You already heard my
6 bio Chair Urban, so I'm just in a dive right in, but of
7 course, being a lawyer I'm going to make sure that we
8 give the typical disclaimer that this presentation
9 reflects my views. It may not reflect the views of the
10 State of California or the Attorney General.

11 I'm going to start by just giving some key takeaways
12 about what I'm hoping this presentation will cover today.
13 I will start by actually reminding the Board that the
14 Attorney General's Office was sitting in the same exact
15 spot as you are now nearly four years ago. We had to be
16 strategic and deliberate about how to craft rules so that
17 they were workable for consumers and businesses alike.
18 We had to contemplate all types of contexts in which
19 consumers would be exercising their rights online and
20 offline, as well as consider small businesses and large
21 businesses compliance.

22 The right to opt out is a critical component of
23 CCPA, and the statutes text require that we focus on how
24 to operationalize this right to opt out. In comparison
25 to the other rights, the CCPA intended stopping the sale

1 of information to be easy. For example, unlike the right
2 to know or the right to delete, the right to opt out is
3 not verified and has very little exceptions. One of the
4 other things that we had heard from stakeholders, which
5 I'll go through today, was about how difficult it was to
6 control the proliferation of their data in the
7 marketplace.

8 I've spoken publicly before about the burden of
9 self-management of one's privacy rights. After all, we
10 are all consumers. Some of us are busy parents. We have
11 multiple jobs and were faced with constant decision
12 making. Figuring out how to control who your data is
13 sold to should not be task intensive or burdensome. And
14 so offering consumers a global option would help
15 facilitate the submission of an opt out request.

16 Lastly, I want to point out that with the
17 regulations in place, the AG actively enforcing this
18 CCPA, including those that pertain to the user enabled
19 global privacy control set forth in the regulations. We
20 have a lot in place. We are going to enforce it.

21 Okay. So I want to start quickly in talking about
22 our goal of operationalizing the right opt out. The
23 Civil Code Section 1798.185, the same provision that's
24 going to guide your rulemaking analysis, required us to
25 promulgate regulations in a whole host of areas. It

1 included subdivision 4(a) and (b), which the language
2 here gave us indication that we had the authority to
3 write rules that facilitated or eased how a consumer can
4 make an opt out request to stop their personal
5 information -- the sale of their personal information.
6 Excuse me. And conversely, we also had to write rules on
7 how businesses had to handle or process requests once
8 they were received.

9 Additionally in the statute, we had broad authority
10 to adopt regulations as necessary to further the purposes
11 of CCPA. We could adopt regulations that filled in the
12 details not specifically addressed by the text of the
13 statute but fell within its scope. So while, for
14 example, the text of the statute set a baseline
15 requirement for businesses that sell personal information
16 to post a "do not sell my personal information" link. It
17 did not foreclose the Office of the Attorney General from
18 also establishing additional mechanisms to facilitate the
19 submission of consumers opt out request.

20 The right to opt out is the hallmark of CCPA. This
21 is something that when we first started our rulemaking
22 process we had to consider, and so we started with the
23 text of the statute. At the outset, you've heard about
24 how CCPA is about consumer rights. Indeed, CPRA, which
25 amended CCPA, now includes the word rights in the title.

1 More importantly, it's about things -- these rights that
2 belong to the consumer which we all are.

3 We approach this this rule making task through the
4 lens of the right rooted in the California Consumer
5 Privacy Act. Not the business mitigating legal risks
6 when selling information act. The text itself was
7 important and critical. You have the right, at any time,
8 to direct. This is forceful and meant to be robust. You
9 also -- the right means to stop selling personal
10 information to third parties.

11 Also within the text were special protections for
12 minors. You cannot sell unless you have permission,
13 either from the minor age 13 to 16, or from the parent or
14 guardian under 13. These were new protections and they
15 were supposed to be meaningful.

16 There's other important clues within the text that
17 guided our analysis of how to draft regulations. For
18 example, it's a clear binary action. Sell or do not
19 sell. Businesses were also required to be transparent if
20 they sold by the law. There's is a requirement to
21 clearly disclose that you do sell, namely by posting the
22 link on your website, as well as putting in your privacy
23 policies.

24 There's also requirements to train employees on how
25 this works. All individuals responsible for handling

1 inquiries are informed of all requirements in 1798.120,
2 and how to direct consumers to exercise their rights.
3 And then finally, the right to opt out should be
4 respected and good for one year.

5 We also considered context. The CCPA is the first
6 law in the nation to vest consumers with this critical
7 right. Fortifying this right so that its meaningful for
8 consumers requires that the Office of Attorney General
9 establish robust set of rules and procedures. Nothing in
10 the legislative history indicated that the legislature
11 intended to limit rulemaking, and the provisions as I
12 said before referred to the section that set forth the
13 rights 1790.120. The right itself and not merely the
14 attendant obligations for compliance.

15 Finally, and something I really would like to share
16 with you is that we listen to stakeholders. There's one
17 particular stakeholder that comes to mind during our
18 pre-rulemaking activities as well. She was named Louise
19 (ph.) and she spoke at one of our meetings in Sacramento.
20 She stuck out to me personally because we wanted to hear
21 from consumers. We had heard from a variety of
22 stakeholders, including industry, about their positions.
23 As so I'm quoting from the transcript that's of that
24 meeting, which is posted on our website, and you could
25 read it. But I'm reading it for clarity and to conserve

1 time. Louise said, quote,
2 "After listening to the comments so far, I am
3 largely here to stay help. I am an educated
4 person, reasonably computer literate. I have
5 never made it all the way through an opt out
6 procedure. They splinter. They go here and
7 there. They require you to log into your
8 account. And then when you get there you don't
9 know the definitions are of what you are opting
10 in or out to. So we need help and we needed
11 from you." End quote.

12 She pointed out that some consumers don't enjoy how
13 the internet relies on their personal advertising -- on
14 their personal information in order to serve
15 advertisements. She noted that there was a large market
16 for something called an ad blocker, which is an extension
17 that a consumer can download and install to their
18 browser. She ended by saying,

19 As you work to implement this law, consider
20 what people can actually see and understand
21 about what's being collected and how it's used,
22 because overall, I think it's been used to our
23 harm in getting a data dump isn't going to
24 help. Thank you for the opportunity, and
25 please remember all of us out there who just

1 don't know what's going on."

2 What I think Louise meant here by things like when
3 she referred to a data dump and her overall confusion,
4 without figuring out how to navigate the opt out process,
5 especially, was complicated, time-consuming, and decision
6 fatiguing. It was our job to make it easier for
7 consumers to advance protecting privacy. It sounded to
8 me like Louise was tired of always being asked are you
9 sure each time she visited a website. And just to echo
10 some of the previous presentations that we've heard
11 today, we know that this is sometimes done through things
12 like deception, or to deter a consumer from taking an
13 action that they intend to do.

14 Lastly, we also relied on our experience as
15 enforcers. I have spoke repeatedly about how I work on a
16 very talented team of attorneys. We've been doing
17 privacy enforcement for a while. We've been on this -- a
18 cop on this beat, and one of the things we've seen is our
19 work and how the laws should be working better for
20 consumers. One of the laws that we've been enforcing for
21 some time now is the California Online Privacy Protection
22 Act, or CalOPPA. It's an important law. It was also a
23 law that was first in the nation and was intended to
24 require robust privacy disclosures and a privacy policy.
25 It was also meant to give transparency and allow

1 consumers to have all the information they needed before
2 they proceeded or opted to use a website or an online
3 service.

4 I'd like to call your attention to this provision of
5 CalOPPA that required a disclosure how an operator of a
6 website responds to web browser do not track signals, or
7 other mechanisms that provide consumers the ability to
8 exercise choice regarding the collection of personal
9 information -- personally identifiable information,
10 excuse me, about an individual consumers online
11 activities over time and across third-party websites or
12 online services. As the primary enforcer of CalOPPA, my
13 team has reviewed thousands of privacy policies for
14 compliance with CalOPPA. And we found that the majority
15 of businesses will write something similar to this. This
16 is the do not track disclosure that companies will make,
17 including the last sentence that simply states, we do not
18 respond to do not track signals. So we may not be aware
19 of or we may be unable to respond to such signals. Put
20 another way, if given a choice, businesses were
21 disclosing that they simply will not comply with a do not
22 track signal, and if they -- given a choice on how to
23 comply, they will choose not to comply with the signal
24 itself.

25 As we discussed in our initial statement of reasons,

1 imposing a mandatory requirement on businesses to process
2 a global signal was something that was necessary to keep
3 from preventing businesses from subverting or ignoring a
4 consumer tool related to their rights. And specifically
5 the exercise of their CCPA right to opt out. If we were
6 going to facilitate the submission of an opt out request
7 by consumers, we were mindful that we had to make sure
8 that businesses were required to respond and effectively
9 comply with the request.

10 This led us to draft regulation 999.315 having to do
11 with request to opt out. Here is the portion of the
12 statute that takes into consideration what is known as a
13 user enabled global privacy control. A user enabled
14 global privacy control is something that includes a
15 browser plug-in or a privacy setting, a device setting,
16 or some type of mechanism that would communicate or
17 signal a consumer's choice to opt out of the sale of
18 personal information is a valid request submitted
19 pursuant to 1798.120.

20 This rule and the entirety of the subdivision uses
21 words to reflect that the right to opt out should be easy
22 for consumers, involve minimal steps, and be complied
23 with as soon as feasibly possible. The global control is
24 exactly that. It's an on or off switch for consumers.
25 It's intended to be for those consumers that are too

1 busy, too distracted, or overwhelmed by all the prompts
2 and boxes, and just want to stop the sale of their data.
3 Making it a global setting is reflected that this right
4 again, is different. It does -- it should be a right
5 that does not require further information from the
6 consumer. And it's a binary on or off, sell or do not
7 sell request.

8 I want to draw your attention to one area in which
9 we contemplated a modification to the regulation and
10 ultimately decided not to include language. That
11 language is reflected in the blue cross out, and I'm
12 going to walk through this a little bit closely. There
13 was a lot of robust commentary on our regulation, and we
14 addressed each and every comment in our rule making
15 documents. Again, the requirement was that that the
16 control was -- that should be developed in accordance
17 with the regulations clearly communicate or signal that a
18 consumer intends to opt out of sale.

19 We contemplated the question also, as proposed by
20 original language, of whether the privacy control should
21 have a default setting, and we heard from both sides in
22 public comment. One side said that the privacy control
23 should not be defaulted on and that defaulting it off
24 would align with consumer choice. Others pointed out
25 that some consumers choose products because they are

1 designed with privacy in mind, and that choice should be
2 expressed via the user enabled privacy control. The
3 latter viewpoint was compelling. The global privacy
4 control did not need specific language -- excuse me. The
5 regulation involving the global privacy control did not
6 need specific language regarding whether the signal
7 should be on or off by default, because it contemplated
8 that consumers may choose privacy by design products and
9 have the control built in and turned on.

10 Let me say this again. So I want to make it very
11 clear. Consumers can choose privacy. Selecting a
12 product that already builds in high privacy protections
13 is a sufficient expression alone that a consumer wants to
14 protect her privacy. After all, why would we write a
15 regulation that would require that consumers have to
16 continuously provide separate consent. Consumers have
17 grown tired of being repeatedly asked are you sure. To
18 address the concern that consumers could be frustrated if
19 a global privacy setting was defaulted on, the remedy
20 here would just be for a consumer to go in and disable
21 their global privacy control, or revert back to the
22 granularity of going website by website and clicking the
23 do not sell my personal information link.

24 Thus, the regulation reflects that selecting a
25 privacy by design product or service is the affirmative

1 choice in of itself for the user to enable an opt out
2 mechanism. Any additional steps are not necessary, and
3 some of these additional steps would even frustrate the
4 consumer who seeks a comprehensive privacy approach.

5 Lastly, I just want to point out our final statement
6 of reasons. We intended to draft the regulations so that
7 it was forward looking. We thought that there would be a
8 new control that could be developed to comply with the
9 regulation. One that would encourage innovation and have
10 technology be used for the good of advancing consumer
11 privacy. The regulation essential to protecting the
12 consumer's right to opt out reflecting the value of a
13 right for consumers who are too busy, or too overwhelmed
14 to use it. Consumers like Louise, but consumers actually
15 also like each of us that don't have the time, energy, or
16 resources to go website by website, browser my browser,
17 for each and every device for themselves and for their
18 families. We affirm that a global choice, an on/off
19 switch when given, it is a good choice to make. And
20 given the ease and frequency by which personal
21 information is collected and sold when a consumer visits
22 a website, consumers themselves should have a similarly
23 easy ability to request to opt out globally. This
24 regulation was approved by OAL after, again, robust
25 discussion during the comment periods in which we

1 considered each and every comment.

2 I'd like to also note that we have been enforcing
3 the regulations. The enforcement date for CCPA began on
4 July 1, 2020. We began enforcing the statute then. And
5 the regulations once they became finalized and approved
6 by OAL in August. On July 1st, 2021, we posted on our
7 website case examples after one year of CCPA enforcement
8 that included notices of alleged noncompliance that had
9 gone out to businesses and other entities. And included
10 in this list this example involving a business that was
11 not processing requests submitted via user enabled global
12 privacy control. Again, we continue to enforce CCPA and
13 all of its provisions, including 1798.120.135 and
14 regulation included in 999.315.

15 We also have engaged in consumer education such as
16 posting on our website about how to exercise all of your
17 rights under CCPA, including the right to opt out and
18 what the user enabled global privacy control means. So
19 again, just to wrap up, I wanted to make sure that these
20 are my key takeaways. Ultimately, we think that
21 consumers should be able to make technology also work for
22 them. They should be able to have the option to flip a
23 switch that tells all businesses to stop selling my data.
24 This provides a critical power dynamic of businesses
25 where selling personal information is the default.

1 Invest consumers with a mechanism to stop the
2 proliferation of their data in the marketplace with a
3 tool that is mindful of the burden's consumer face with
4 the self-management of their privacy. The CCPA's
5 requirement of a do not sell link on every website was a
6 great start, but having a global option is a critical
7 mechanism to facilitate the submission of request to opt
8 out. It is encouraging to see innovation in the privacy
9 by design space, as well as businesses and even other
10 states that are taking their cues from the groundbreaking
11 work done here in California. An opt out preference
12 signal should be something that is available to all
13 consumers and that is easy, streamlined, and minimal.
14 For companies that are not implementing and building
15 processes to comply with the regulations and the law, we
16 are enforcing. And this is something that we also know.
17 Businesses are speaking to one another and attorneys have
18 commented to us that receiving enforcement notices have
19 been effective towards compliance. We will continue to
20 enforce this regulation and the entirety of CCPA to
21 protect and advance consumers privacy rights.
22 Thank you very much.

23 **MS. URBAN:** Thank you very much, Ms. Schesser. And
24 thank you to all of our speakers today for sharing their
25 deep expertise with us.

1 As a reminder our guest presenters view should not
2 be taken as the views of the Agency or the Board. They
3 are the presenter's views only. That said, I really,
4 very much appreciate the care with which all of our
5 speakers today presented some complex topics. And I
6 think that we will find it useful and hope that others do
7 too.

8 Thank you to everyone who has joined us today and
9 continues to join us. We are going to now welcome public
10 comment. As I mentioned we would do at the end of the
11 presentations today. For those of you who don't need
12 this, please bear with me. I just want to be sure it's
13 clear for everyone. If you want to speak on an item,
14 please use the raise your hand function which can be
15 found in the reaction feature on the bottom of your Zoom
16 screen. Our moderator will request you unmute yourself
17 for comment. And when your comment is completed, the
18 moderator will mute you again.

19 It's helpful if you identify yourself, but of course
20 entirely voluntary. You do not have to. A reminder of
21 the rules of the road. Please keep your comments to
22 three minutes, which is the limit, to make sure that
23 everyone has the same amount of time. And Bagley-Keene
24 does require that comments be connected to the agenda
25 item. So please feel free to plan a comment on topics on

1 any of today's presentations, and to think about that as
2 your topic.

3 I also wanted to note that -- to please realize that
4 the Board cannot generally respond, but please don't
5 think were not listening. All information, including all
6 public comments, are being recorded and transcribed as I
7 mentioned earlier. And will be available for the Board,
8 the staff, and the public to review. And if you have any
9 questions at all, please do write and forward it
10 CPPA.ca.gov.

11 With that, thank you everyone who is considering
12 commenting, and I will ask Mr. Gourley, is there a public
13 comment from anyone in the audience at this time?

14 **MR. GOURLEY:** Yes, Chairperson Urban. We have a
15 few. So I will start with Terry (ph.). You now have
16 permission to unmute yourself.

17 **MS. URBAN:** Mr. Gourley, do you want to try unmuting
18 Terry?

19 **MR. GOURLEY:** Yes, I've asked him to unmute.

20 **MS. URBAN:** Okay.

21 **MR. GOURLEY:** Terry, you have permission to unmute
22 yourself.

23 **MS. URBAN:** All right. Mr. Gourley, I suggest that
24 we move on to the next person then circle back just in
25 case our first commenter walked away and needs to walk

1 back.

2 **MR. GOURLEY:** Okay. Sharon (ph.) you now have
3 permission. Thank you.

4 **FEMALE SPEAKER:** Thank you. Thank you for that. I
5 wanted to give a little bit of feedback. I know we have
6 special protections that we've vindicated for an opt in
7 if they're age persons under 16. I think we need to do
8 that for seniors as well over certain age or whatever,
9 because I think there's another problem with technology.
10 There's a problem with protecting us and we are
11 vulnerable population. So I'd like to see that being
12 considered.

13 Another question - another comment I'd like to make
14 is I'm a little confused how analytics play into it
15 verses a broker. So that something that I'm trying to
16 work out an understand a bit better. And then the
17 problem was if there's a speaker on it that's fabulous,
18 but they may be speaking too quickly, I've no way to make
19 any comments about that, you know, hey, could you slow
20 down a little whatever.

21 So this is my first time of going to this thing.
22 I've stayed with you for the entire thing. I've learned
23 a lot of information, but it's not a style that's
24 user-friendly for a consumer. It's set up for Board
25 members. It's not set up for me to go head and say hey,

1 can you clarify that or do whatever. So I just wanted to
2 share that information.

3 And then that this wonderful research that's being
4 done, it's great. And yet am worried that the companies
5 are going to use that information to modify, we'll, hey,
6 we can hold 15 seconds, but we can use 10 seconds. So
7 I'm saying is it's a double-edged sword that research is
8 being done can also be used for the people that want to
9 manipulate us. And I just wanted to get that out there.
10 Thank you.

11 **MS. URBAN:** Thank you very much, Ms. Vasquez (ph.),
12 and for your question earlier today. Thank you. Much
13 appreciated.

14 Mr. Gourley, is there another commenter?

15 **MR. GOURLEY:** Yes, Jennifer, you now have
16 permission. You can unmute yourself.

17 **MS. HUDDLESTON:** Thank very much and thank you for
18 this time. My name is Jennifer Huddleston, and I am
19 policy counsel with Net Choice, a trade association
20 dedicated to keeping the Internet safe for free
21 enterprise and free expression.

22 I just wanted to make a comment regarding some of
23 the information that was presented today that the CCE --
24 the CCPA should be careful when it's considering how to
25 go about rulemaking not to regulate the beneficial uses

1 of algorithms and a desire to define dark patterns and
2 avoid what it considers harmful uses.

3 Beneficial algorithms are very helpful in making our
4 experience online much better, including helping us to
5 avoid spam, and underpin many of the services that make
6 the internet the way it is today. Additionally, any
7 rulemaking that the CPPA focuses on should focus on those
8 issues that are related to privacy. Often times there
9 are trade-offs that need to be carefully considered when
10 it comes to user speech and issues like content
11 moderation. And the Agency should be careful to ensure
12 that it's staying within its mandate to focus on privacy.
13 Thank you.

14 **MS. URBAN:** Thank you very much, Ms. Huddleston.

15 Mr. Gourley, are there further commenters?

16 **MR. GOURLEY:** Yes. Cecilia you know have permission
17 to unmute yourself. Thank you.

18 **MS. NEWMAN:** Thanks so much. I simply wanted to
19 thank the Board and the Agency for putting this
20 presentation together. I joined -- I'm a privacy
21 professional. I joined the presentation thinking that
22 this was an information about the -- you know, I wasn't
23 well-informed about today's session. But I have a very,
24 very, happy to see what was presented today. The
25 information provided was extremely informational and

1 insightful, and I just want to thank everyone that put
2 this together. That was my comment. Thank you.

3 **MS. URBAN:** Thank you very much, Ms. Newman, and I'm
4 sure everyone who worked on it greatly appreciates that.

5 **MR. GOURLEY:** Okay. Maureen, you know have
6 permission.

7 **MS. MAHONEY:** Chair, members of the Board, thank you
8 for the opportunity to speak today. My name is Maureen
9 Mahoney of Consumer Reports. I very much appreciate the
10 presentations and wanted to take this opportunity to
11 highlight a few issues we think are important with
12 respect to the rulemaking.

13 In our view, consumers privacy should be protected
14 by default through strong data minimization that
15 prohibits all unnecessary data processing. So that
16 consumers can use online services safely and apps safely
17 without having to take additional action. But at the
18 very least, measures based largely on an opt out model
19 like the CCPA should be workable for consumers and the
20 new regulations should clarify that business are required
21 to honor browser privacy signals, as not data sharing
22 itself consistent with the plain language of CPRA and
23 consistent with existing AG regulations. And without
24 this, consumers will have few options but to opt out at
25 every company, one by one, even though there are

1 hundreds, if not thousands, of companies that sell
2 consumer data.

3 Second, it's important to make sure that the opt out
4 as comprehensive. We urge the agency to help ensure that
5 when the consumer opts out, companies can't make their
6 personal information available to third parties for
7 commercial purpose. We found that some companies have
8 ignored the opt out with respect to behavioral
9 advertising under the CCPA. And sent some consumers to
10 ineffective third-party industry opt outs which
11 undermines the purpose of the law.

12 CPRA takes steps to help address this, including an
13 opt out of sharing be given by bad faith interpretations
14 of the CCPA, I think it should be reiterated that
15 retargeting, in particular, is covered by the CPRA opt
16 out. All this will help ensure that consumers are easily
17 able to exercise her privacy preferences. One of the key
18 goals of the law. Thank you, again.

19 **MS. URBAN:** Thank you, Ms. Mahoney. Mr. Gourley,
20 are there further public commenters?

21 **MR. GOURLEY:** Yes. We have another one. Angelina
22 (ph.), you know have permission.

23 **MS. LOAS:** Hi.

24 **MS. URBAN:** Oh dear. Mr. Gourley, do we still have
25 Ms. Loas? There she is. All right. Ms. Loas, apologies

1 for that. Please do go ahead. I think you can talk now.

2 **MS. LOAS:** Okay. No worries. So thank you all so
3 much for putting this together. It was quite helpful to
4 be able to identify the use cases that are contemplated
5 under the CPRA. I know that there's been just a lot of
6 kind of confusion around those.

7 One thing that I would like to suggest is to have a
8 bit more clarity on the interplay between the CCPA, CPRA,
9 and COPPA. I understand that there's a preemption, you
10 know, clause in the CPRA, you know, saying that it really
11 supplements and should not conflict with COPPA. And I
12 think that's true with regard to opt into collection
13 that's quite clear and with -- to a two to a certain
14 extent with the opt out of sales required verifiable
15 parental consent for minors, etcetera. But I think
16 that's not so clear with regard to the opt outs. And I
17 think with, you know, "do not share" for cross context
18 limit the use of -- limit the use and disclosure of my
19 sensitive PI. I think it's unclear whether verifiable
20 parental consent will be needed. You know, kind of what
21 approach should entities or businesses take with regard
22 to children exercising those opt outs versus adults. I
23 think we would just need a bit more clarity around that.

24 **MS. URBAN:** Thank you very much, Ms. Loas.

25 Mr. Gourley, do we have remaining public commenters?

1 **MR. GOURLEY:** Yes. We have one more. Leo, you now
2 have permission to unmute.

3 **Mr. HWANG:** Hi. I'm Leo. I'm a UCLA's third-year
4 law student and focus on technology law. Thank you,
5 first of all, for this panel. It was really informative.
6 I have -- so my comment would be on at OCC -- the CCPA
7 requires business to maintain reasonable security
8 practices in order to shove them from liability in the
9 event of data breeches. But the study do not define what
10 constitutes reasonable security. So currently, what
11 business do is that they look Federal guidelines as their
12 statement. NIST frameworks for recommendations to
13 demonstrate that reasonable security practice. However,
14 the guidelines are really, like, voluntary and is not
15 effective.

16 So the law will not achieve its goal until this --
17 there's a mandate to tell what the companies should do to
18 actually have teeth to achieve the goal of protective the
19 data of the customers. And that goes back to the panel.
20 What the panel said about the dark patterns that how
21 easily usually and fragile the customers can be, and how
22 manipulative the -- those techniques could be.

23 So if the Agency could make clear of the definition
24 of reasonable security in that statute it would be
25 greatly appreciated by the industry and the academic, as

1 well. Thank you.

2 **MS. URBAN:** Thank you much, Mr. Hwang. Mr.
3 Gourley, do we have further public comment?

4 **MR. GOURLEY:** There is no further comment at this
5 time, Chairperson Urban.

6 **MS. URBAN:** Thank you, Mr. Gourley. As before, I
7 will wait just a little while in case anyone's
8 formulating thoughts. So we'll give it a minute or so.

9 All right. My deep gratitude to everyone who took
10 the time to comment during public comment, and again to
11 our speakers for today. We will now recess until 9 a.m.
12 tomorrow March 30th. And we will continue with the pre-
13 rulemaking information sessions.

14 If you want to see what topics are coming up, that's
15 on the agenda for day two, and I just emphasize that
16 because we started at 11:00 today, tomorrow we're
17 starting at a different time at 9: a.m. And we hope to
18 see anyone is interested there.

19 Thank you very much. We are now in recess.

20 (End of recording)

21

22

23

24

25

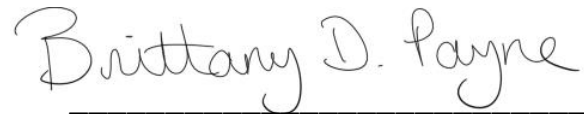
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

TRANSCRIBER'S CERTIFICATE

STATE OF CALIFORNIA

This is to certify that I transcribed the foregoing pages 1 to 157 to the best of my ability from an audio recording provided to me.

I have subscribed this certificate at Phoenix, Arizona, this 24th day of April, 2022.

A handwritten signature in cursive script that reads "Brittany D. Payne". The signature is written in dark ink and is positioned above a horizontal line.

Brittany D. Payne

eScribers, LLC

--o0o--