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

--o0o--

**TRANSCRIBED RECORDED PUBLIC MEETING**

**March 29, 2022**

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

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

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

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

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

**MR. LE:** Present.

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

**MS. SIERRA:** Present.

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

**MR. THOMPSON:** Present.

**MR. GOURLEY:** Chairperson Urban.

**MS. URBAN:** Present.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

have up to three minute to make your comment.

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

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

**MS. URBAN:** Okay.

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

**SHARON:** Thank you. Could you do me a favor and clearly define what a stakeholder means? I'm unmuted.

**MS. URBAN:** I would suggest that you go to the website and read more information about the sessions, but anyone who has an interest in the topics under the agency's jurisdiction.

**SHARON:** Okay. Great. So us persons participating in this meeting this morning or listening into this meeting are considered stakeholders?

**MS. URBAN:** Sure.

**SHARON:** Thank you.

**MR. GOURLEY:** Thank you.

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

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

**MS. URBAN:** Okay. Let's just wait for a little while and see if people are formulating thoughts, and then if not, we will go to the next item.

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

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

And thank you for the public comment we received.

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

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

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

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

flows for us today.

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

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

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

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

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

the common data flows to help ground further discussion.

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

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

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

Like the retail example, these data are typically

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

The previous slide showed the perspective of one

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

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

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

Some of these uses might be to identify potential

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

To overlay this right to delete with regard to the

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Again, from or experience and from consumer complaints, there are some con -- there are some barriers that consumers may commonly face with regard to the exercising of this right. Sometimes businesses are not clear with regard to their representation that they do not sell personal information when in fact they do. There's also an issue where even though this right, no verification is needed to exercise this right, oftentimes

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(Whereupon, a recess was held)

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

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

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

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

get them processed and up on the website.

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

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

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

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

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

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

Hi, Professor Strahilevitz. Thank you for joining us.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

users to do the things they would not otherwise do.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

you've been exposed to.

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

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

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

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

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

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

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

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

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

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

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

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

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

very carefully designed.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

decision that the coercing party wants you to make.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

dark patterns that highlighted their prevalence, their increasing prevalence.

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

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

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

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

Times poll.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

If they clicked other options, then they were going

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Okay. So we were really intrigued by this first set

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

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

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

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

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

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

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

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

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

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

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

prominent.

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

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

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

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

but they could accept it right away.

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

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

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

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

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

acceptance rate all the way up to 22.1 percent.

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

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

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

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

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

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

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

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

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

be highly significant.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

consumer welfare.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

And thank you so much.

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

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

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

2:18 p.m. for the rest of this afternoon's presentations. And again, thank you very much.

(Whereupon, a recess was held)

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

And are we still recording?

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

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

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

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

and Consumer Preferences.

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

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

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

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

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

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

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

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

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

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

the number might even actually have gone up.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Now, you can see we still had a lot of

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

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

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

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

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

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

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

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

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

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

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

Okay. So for our first evaluation, we did this

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

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

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

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

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

a lot of misconceptions associated with it.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

simplify things.

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

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

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

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

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

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

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

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

the impact would be.

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

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

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

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

higher motivation to click on the link.

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

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

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

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

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

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

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

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

meter?

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

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

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

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

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

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

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

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

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

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

their privacy policies very easily.

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

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

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

And what we found in our user studies is that this

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

be able to use another one.

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

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

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

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

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

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

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

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

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

what I was actually confirming.

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

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

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

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

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

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

We had over a thousand participants in the study.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

Ms. Schesser, welcome and the floor is yours.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

time. Louise said, quote,

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

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

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

don't know what's going on."

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

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

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

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

As we discussed in our initial statement of reasons,

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

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

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

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

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

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

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

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

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

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

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

considered each and every comment.

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

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

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

Thank you very much.

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

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

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

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

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

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

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

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

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

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

**MS. URBAN:** Okay.

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

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

back.

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

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

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

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

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

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

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

Mr. Gourley, is there another commenter?

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

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

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

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

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

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

Mr. Gourley, are there further commenters?

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

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

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

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

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

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

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

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

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

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

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

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

**MS. LOAS:** Hi.

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

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

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

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

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

Mr. Gourley, do we have remaining public commenters?

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

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

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

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

well. Thank you.

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

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

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

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

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

Thank you very much. We are now in recess.

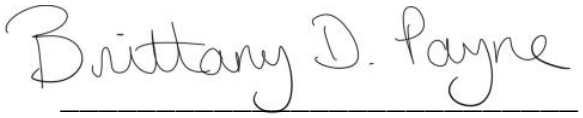
(End of recording)

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.



Brittany D. Payne

eScribers, LLC

--o0o--