MEETING OF THE

CALIFORNIA PRIVACY PROTECTION AGENCY

(Pages 1 - 137)

Location: Cannabis Control Appeals Panel Hearing Room, Suite 330
400 R Street Sacramento, CA 95811

Date: Thursday, April 30th, 2026

Transcribed by: Samuel Murry

APPEARANCES:

BOARD MEMBERS (IN PERSON):

Jennifer M. Urban - Chairperson

Drew Liebert - Board Member

Jill Hamer - Board Member

Nicole A. Ozer - Board Member

BOARD MEMBERS (VIA ZOOM):

Alastair Mactaggart - Board Member

Serena Carwile - Moderator

PRESENTERS (IN PERSON):

Jacob Snow - Senior Staff Attorney, ACLU of Northern California

Nathan Good - Founder & CEO, Good Research

PRESENTERS (VIA ZOOM):

Rebecca Kelly Slaughter - Former FTC Commissioner

Richard Salgado - Principal Member, Salgado Strategies, LLC

Tom Bowman - Policy Counsel, Center for Democracy and Technology

Madeline Dwyer - Policy Analyst, Center for Democracy and Technology

David LeDuc - Vice President of Public Policy, Network Advertising Initiative

PROCEEDINGS

CHAIR URBAN: Good afternoon. Welcome to the California Privacy Protection Agency's informational session and board hearing. We will be holding these over the course of; today, April 30th, 2026; and tomorrow, May 1st, 2026. We are meeting in Sacramento.

I'm pleased to be here today and tomorrow with my fellow Board members in person and virtually, and I welcome members of the public here in person and many of you joining us via Zoom. Before we get started, just a few quick reminders. Please make sure your microphone is muted when you are not speaking.

If you are here in-person, please silence your cell phone to avoid interruptions. And importantly, please note that this meeting is being recorded. The meeting is in a hybrid format. Four -- four -- of my -- of our Board are here in person, as well as members of the agency staff, and Board member Alastair Mactaggart is joining us remotely.

Both days of this meeting of the Board will follow the Bagley-Keene Open Meeting Act as required by law. The agenda and supporting materials are available here in Sacramento and on the CPPA website. You may

notice Board members accessing their laptop screens or other devices during this -- during the meeting. They are using these devices solely to access board meeting materials.

The Board always welcomes public comment, and I will call for it this afternoon at the end of our informational program. Tomorrow morning, I will provide more detail about public comment on the agenda items for that day.

Please do note the general rules for public comment. Each speaker will have up to three minutes to make their comment, and under the Bagley-Keene Open Meeting Act, both Board members and members of the public may only discuss items that are listed on the agenda.

For this afternoon's program, that means that public comment should relate to topics discussed on the program this afternoon. Members of the public will have an opportunity to comment either via Zoom or in person, and I will provide more detail about participation when we reach the time for public comment.

Please note that the hybrid format creates technical complexities, and please bear with us if we experience any technical issues. If that happens, we will pause the meeting and address them as needed. If you're attending remotely and something happens such that you

experience technical issues like the audio dropping, please email info@cppa.ca.gov. That's India November Foxtrot -- excuse me, Oscar -- @CaliforniaPrivacyProtectionAgency.ca.gov.

The inbox will be monitored throughout the meeting. We will take breaks as needed. I will, though, be moving things along as we have a very rich program today. My thanks to the Board members for their service and to everyone helping make today's meeting possible. My special thanks to Executive Director Tom Kemp and Philip Laird, General Counsel, who are serving in their capacities with us today.

I'd like to welcome our moderator, Ms. Serena Carwile. Thank her also for managing the technical side of today's meeting and ask her now to please conduct the roll call.

MS. CARWILE: Board member Hamer?

MS. HAMER: Present.

MS. CARWILE: Board member Liebert?

MR. LIEBERT: Here.

MS. CARWILE: Board member Mactaggart?

CHAIR URBAN: He has his hand up and I can see him. I'm going to say he's here.

MR. MACTAGGART: I'm here.

MS. CARWILE: Board member Ozer?

MS. OZER: Present.

MS. CARWILE: And Chair -- oh, sorry, Chair Urban?

CHAIR URBAN: Present.

MS. CARWILE: Madam Chair, you have five present - or, sorry -- we have four here and one virtual.

CHAIR URBAN: Thank you very much, Ms. Carwile. The Board has established a quorum. Before we begin with the program itself, I will take a moment to explain the format for this informational session.

This is the first in what we expect to be a series of public informational sessions to assist both the board and the public in learning about topics that are relevant to the Agency's work. This afternoon's informational session is on the Private to Federal Pipeline: How Federal Agencies Use Private Data and How States Can Protect Americans.

We will hear from a panel of expert presenters who will provide background on the issues before us and offer a range of perspectives for consideration. Our speakers include a federal official, a technology expert, academics who study relevant areas of law, and members of civil society groups and the business community.

I want to emphasize that the views presented by our guest speakers are their own. They should not be

taken as the views of the Agency or the Board.

I will introduce each speaker with a brief biography before their presentation. Speaker biographies and any slides used today will be posted on our website as soon as they can be processed.

We are here today to examine and consider a serious, indeed urgent, moment in our civic life. Several developments are occurring simultaneously that raise profound concerns about the privacy of individuals, including the underlying values of due process, democratic transparency, and human dignity that connect to privacy.

These developments also raise questions about the role of states in protecting these fundamental democratic values. First, we are witnessing what a real-time betrayal of public trust by the federal government with respect to personal data held and processed by federal agencies looks and feels like.

The federal government collects some of the most sensitive information there is about us. For example, the Treasury Department collects and stores tax data that includes details about income, family structure, location, charitable contributions, Social Security numbers, and birth dates.

The Social Security Administration collects work history and income, age, detailed health information for

many people. Indeed, so much information that the Social Security -- its Social Security number and accompanying information are the basis for the identification systems in the United States, both public and private. These are just two examples from agencies familiar to both of us. Americans have always had the expectation and the right to expect that this information was held in trust for use to benefit Americans through the important programs agencies administer.

For decades, personal data collected by the federal government has been protected by laws such as the Privacy Act of 1974 which provides transparency, accountability, and protections around the collection, use, and sharing of personal information by federal agencies. It is important to acknowledge that the twin forces impelling the Privacy Act's passage were first, a recognition that federal databases posed both a promise and a threat to the American people; and second, a severe breach of trust by the Nixon administration and prior administrations by surveilling the populace.

However, these protections are now under attack. We are seeing instances in which these laws are being ignored, and information is being shared among agencies and outside entities in ways that appear to violate these legal protections. Second, we are seeing the rise of

federal enforcement authorities acquiring personal data from corporate entities, including data brokers, to track and profile individual.

Data brokers buy and sell vast quantities of information from mobile apps and browsers that can reveal intimate details about people's daily lives. Agencies such as the FBI and DHS regularly purchase such data from data brokers. This information can then be used to profile individuals, target people for immigration enforcement, and access personal details that would otherwise require a warrant supported by probable cause.

This circumvents fundamental constitutional privacy and due process rights. It also shrouds enforcement activities in secrecy, where warrants would otherwise provide transparency into the government's enforcement practices. Unfortunately, existing federal law appears not to restrict or limit this practice.

And finally, in the midst of this extensive collection of data and misuse and sharing of information by the federal government, we are facing increased federal efforts to preempt state privacy protections for our residents. Recent executive orders, proposed legislative frameworks, and federal bills have advocated for broad preemption of state laws related to consumer privacy, online protections for children and teens, and basic

safeguards around artificial intelligence.

These actions raise a host of questions about those fundamental democratic values and how they are being served, and ultimately about the role of states and how states, including California, can help preserve and defend democratic values and work to ensure that those values and privacy protections that give them force continue to protect our residents.

Today we're going to hear from experts who can provide background on what is happening, what guardrails are in place, what role states can play, and how businesses have approached these issues. It is our hope that this session will help us explore and consider the scope of changes at play to support our analysis of the role states can play and support our ongoing analysis of the potential role we have within our authority as a state privacy agency.

We will hear from experts in three stages. First, Federal Trade Commissioner Rebecca Slaughter will provide an overview of the existing federal framework for consumer data, some -- a strain that it's under, and her view from D.C. on states' role in protecting privacy.

Next, we will hear from experts Rick Salgado and Nathan Good. Mr. Salgado will provide an overview of federal acquisition of information via legal process, that

is the traditional path. Dr. Good and his partner, Ms. Chen, will provide an overview of data flows in the AdTech marketplace and where unexpected data flows may appear. Third, we'll hear from a panel of policy experts and advocates who will provide further factual background and some viewpoints on potential policy approaches.

I will pause after each stage and invite board members to ask questions of the presenters or to comment. Staff will keep -- help me keep an eye on the overall time, and I'll flag any need to wrap up for that section. I'll ask board members to hold questions until we finish the stage so that we ensure we have time for the full richness of the program today. I will request public comment after we and members of the public have had the opportunity to hear from all speakers.

Before we move to our first presentation, I want to thank all of our speakers for taking the time to be with us today and to thank everyone working behind the scenes to make this meeting possible. My thanks as well to our board members for their service.

We will now proceed to our first stage of presentations, Federal Access to Commercial Data: Existing Federal Framework and the Role of States, with our speaker, the Honorable Rebecca Kelly Slaughter, Commissioner for the Federal Trade Commission.

MS. SLAUGHTER: Thank you so much, Chair Urban, and thank you so much for the invitation to be here. It's really an honor to get to present to this esteemed group, and I'm grateful for your attention to these incredibly important matters. I'm going to try to share my screen, so let me get that set up.

Here we go. Okay. Can you see that? We good?

CHAIR URBAN: We do not see it yet. There we go. Here -- okay.

MS. SLAUGHTER: Okay, great. Great. Okay. So I want to start with a sort of dire warning that we are at a moment where privacy is truly in peril because unchecked commercial surveillance has collided with unbalanced executive power. Let me tell you a little bit about the perspective from which I'm speaking.

As Chair Urban mentioned, I have been a commissioner on the Federal Trade Commission. I was appointed in 2018, actually by Donald Trump originally. I served as the acting chair in 2021 at the beginning of the Biden administration and went on to be majority Commissioner in the Biden administration and resumed my position as a Minority Commissioner at the beginning of the second Trump administration until President Trump tried to remove me at the beginning, or in the middle of March of 2025.

I challenged that removal, and that case is currently pending at the Supreme Court. It was argued in December, and it could be decided any day.

Before I came to the FTC, I served as Chief Counsel to Senator Schumer from New York, the Democratic leader, for a long time, where my portfolio included issues of privacy and competition, and technology generally. So I have a deep background on both the legislative and administrative aspects of federal law here.

And from that background, I mentioned both the Supreme Court case and my FTC work because I am sitting in a unique perspective. I have two substantive background areas of law here, privacy and competition on the one hand, and then as a litigant, admin and constitutional law. And so my perspective is really born out of how those two things interact, and it has led me to the conclusion that when unchecked commercial surveillance is combined with unbalanced executive power, we have not just two separate problems, but a mutually reinforcing crisis.

Because a president who controls -- oh, sorry, one second, let me go back -- a president who controls agencies and allies with dominant platforms can get comprehensive data on all Americans pretty much without a warrant. And that means that states and private

enforcement are really an even more essential backstop than they have been in the past.

So let's talk about commercial surveillance, generally. I think we are all very familiar, California more familiar maybe than anyone -- any other state -- with the concept that the general notice and consent framework benchmark for data access is really both outdated and ineffective to protect Americans from the kinds of harms that can be born out of unfettered data collection and use.

As you know better than anyone, we don't have a federal privacy law in the United States. What we do have is the FTC Act. I'll just give you a brief overview of what it protects and how it applies in this context.

The FTC Act primarily prohibits unfair deceptive acts and practices. It also prohibits unfair methods of competition, but that's less relevant to this case. Unfairness has a statutory three-prong test. For something to be an unfair act or practice, it must cause substantial injury that's not reasonably avoidable and not offset by countervailing benefits to consumers or competition.

Deceptive is pretty much straightforward. It means lying about commercial behavior, including data collection and use.

We also enforce COPPA, the Children's Online Privacy Protection Act, which primarily operates to require verified parental consent for access to children's data. It has some underutilized provisions on minimization as well. There are a few other statutory frameworks that apply in the privacy context, the Health Breach Notification Rule and the Safeguards Rule, but the FTC Act and COPPA are really the primary, primary protections.

I want to point your attention as you're engaging in this inquiry and study to the rulemaking record that the FTC developed during the Biden administration under Chair Khan's leadership on data security and commercial surveillance. That has not evolved into rules, but the record itself is an incredibly rich and valuable resource with perspectives from industry, academia, civil society, other enforcers. And I really encourage you to dig into it and think about whether it provides some of the answers to some of the questions that you have.

The FTC has been doing enforcement in the privacy context under these general framework rules for a very long time. And in my time there, we brought a number of cases, including many cases against, I think, data privacy cases against almost all the large platforms. I'll point your attention in particular to the cases against Facebook

and Meta that started in 2011.

We had the order violation case in 2019 that was associated with Cambridge Analytica data collection, and then a 2023 proceeding alleging further ineffectiveness of that order. We brought cases against Amazon related to both Alexa and Ring, getting a $25 million penalty for COPPA violations related to Alexa's collection of children's voice data, which was done in order to train AI models, voice recognition AI models, and another penalty for illegal access to Ring videos.

We brought a case against Google and YouTube in 2019 with a $170 million civil penalty for COPPA violations related to child-directed content on YouTube. And there have been many smaller cases as well.

I think it's important to note that platforms are not the only problem here in the data universe. Smaller companies do not mean a smaller risk. So I want to call attention to three recent data broker cases that -- that go directly to the commercial collection of sensitive data, some of which has been accessed by the federal government.

So the first case involved Gravy Analytics and Venntel. It involved the collection of 17 billion location signals per day from over a billion devices, and the company would apply 1,000 different behavioral labels

per consumer. They tracked things like religious attendance, showing up at reproductive healthcare clinics or political rallies.

And this data was sold not only to other private companies, but also to federal agencies, including the Department of Homeland Security, the DEA, the FBI, and the IRS.

We also brought a case against Mobilewalla, which sold raw location data via real-time bidding without any meaningful consent verification. Mobilewalla tracked individuals at military bases, domestic violence shelters, and union organizing events, and it built demographic profiles of racial justice protesters in 2020.

There's an ongoing litigation against the data broker Kochava, which has passed the motion to dismiss stage. Kochava, the FTC alleged, collect a staggering amount of sensitive identifying info, including precise geolocation and names, email, phone, income, ethnicity, political affiliation. And according to the District Court that analyzed the FTC's case, the company was selling encyclopedic information in a way that could plausibly cause substantial injury, and that the privacy invasion itself could amount to a substantial injury.

And that case is important because it was brought not as a deception case, which is the basis for a lot of

the privacy cases the FTC has brought, including the Facebook-Cambridge-Analytica-associated cases, it was an unfairness case. So the allegation was just the collection and use of this data could cause substantial injury that's not reasonably avoidable and not offset by countervailing benefits.

I think the point about bringing up these cases is that these are not one-offs and they are not unusual. This is what happens in an economy and a business model where there is a commercial incentive to collect unlimited amounts of data and monetize it, and there is no meaningful legal backstop that would make -- that would disincentivize that collection by making it illegal or making violations of the law unprofitable.

I want to draw attention to the fact that it's not just the collection and it's not just the big companies. It is actually the fact that there are now large companies who have data on almost every American, if not every American. This is a problem for three reasons. First of all, it means avoidance is impossible.

In a competitively healthy market, if consumers did not like the data practices of a particular company, they could patronize rivals of that company. But when two or three firms control everything necessary for modern life, it's not realistic to imagine that consumers can

take their business elsewhere.

Kash Hill did an amazing job documenting this with a series of articles in which she described how she tried to quit Big Tech and it was impossible for her to do so. And I think this is part of the reason we can understand that notice and consent doesn't particularly work because consent is not meaningful if it cannot -- if you cannot choose not to participate in a particular data ecosystem. The other problem --

CHAIR URBAN: Commissioner Slaughter.

MS. SLAUGHTER: Oh yeah, so go ahead.

CHAIR URBAN: I really apologize. We are incredibly appreciative that you have taken the time to join us. We are actually having connectivity issues.

MS. SLAUGHTER: Oh no, I'm so sorry. Is it on my end?

CHAIR URBAN: It is definitely not on your end. Incorrect information was posted online in terms of the link the public can use. So we actually need to pause the meeting for a few minutes while the correct information is provided. I really do apologize.

MS. SLAUGHTER: Oh, don't worry about it. I'm happy to pause.

CHAIR URBAN: It's a riveting presentation.

MS. SLAUGHTER: Okay. I'm happy to pause.

(Whereupon, the proceeding was interrupted by a technical issue.)

CHAIR URBAN: Okay. Thank you so much. All right, welcome back everyone. Again, with many thanks for your patience while we dealt with the technical issue. The correct link to the meeting should now be posted anywhere on our website so that you can find it along with the notice, an explanatory notice.

We have a couple of speakers who are very tight for time, our first two speakers. And so I'm going to ask -- I will keep an eye on time and I will help us all sort of get through it so that we are able to hear from both of you and you're able to hear from the Board.

And with that, I will ask Commissioner Slaughter, please do continue. It was a riveting presentation, and I'm happy to be riveted again.

MS. SLAUGHTER: Okay. I think I have my screen back up. I want to confirm that you can see it, Chair Urban.

CHAIR URBAN: Yes, we can. Thank you.

MS. SLAUGHTER: Great. Okay, terrific. So we were talking about why the issue is not just data collection, but actually also market concentration that

becomes a problem here. I made the point that avoidance is impossible where you have concentrated data markets. There's also no competitive discipline. Firms are not incentivized to fix their practices because they're afraid of a competitor swooping up their customers. So privacy violations can then become economically rational for these businesses.

And I think the most important point that I would make is that concentration creates catastrophic single points of failure. So when data is diffused among many different entities, then any single breach only exposes the data that is held by that entity. But when data is concentrated into single actors, then one breach exposes the entire population. So you have concentration converting data from a distributed risk into a systemic one.

Okay. Now let's talk about executive power. Executive power and privacy go hand in hand with some of this conversation about commercial surveillance. We have two federal agencies that operate to oversee privacy issues in different ways. The one is the FTC, which handles commercial surveillance, and the other is the Privacy and Civil Liberties Oversight Board, which oversees executive access to government access to data, especially from a national security perspective.

Both of these agencies were established by Congress with removal protections for their commissioners. Specifically, in statute at the FTC, the commissioners cannot be removed other than for neglect, inefficiency, and malfeasance.

That was true when Congress set up the agency in 1914, and it has been unchanged in the intervening years. It was challenged one time by President Roosevelt in 1933 when he tried to remove Commissioner Humphrey, ironically because Commissioner Humphrey, a conservative Republican, was interfering with the Roosevelt administration's implementation of the New Deal, and President Roosevelt tried to remove Commissioner Humphrey.

Commissioner Humphrey would not accede to that removal. He sued challenging the removal, and he died, but his estate continued the lawsuit, and the resulting case in front of the Supreme Court was Humphrey's Executor, which was a unanimous 9-0 decision that said that for-cause removal protections at independent boards and commissions were constitutional.

Why are they important at agencies like the FTC and the PCLOB, and for what it's worth, a variety of other agencies that protect market integrity in various ways? Because to do privacy enforcement from a commercial perspective, the FTC has to take on some of the most

powerful and politically well-connected actors in our economy.

And the for-cause removal protections ensure that decisions are made on the merits, on the facts and the law of the case. And the way I think about it is that it ensures that agency decisions are made without fear or favor, specifically without fear of getting fired for failure to do a favor for the President's friends or allies.

So by removing even just the minority commissioners at the FTC and the PCLOB, the President sent a message that he's willing to remove all commissioners if they don't do exactly what he wants for political reasons, not in accordance with the law. And that creates a chilling effect on enforcement. It doesn't even have to be explicit. It's just the sort of sword of Damocles hanging over a commissioner's head.

And the other reason it's really important is that what independence provides, and multi-member bipartisan boards provide, is not, first a drive towards consensus, which I think is positive for the law in the -- in the long run and the short run and the body politic; they also provide transparency and accountability into agency decision-makings.

So for example, when I dissented on the Facebook

$5 billion settlement that I mentioned earlier, I thought it was ineffective, but I didn't think it was done for politically inappropriate reasons. I just thought it wouldn't work. If I had thought it was the object of political pressure or corruption, I would have said that. And so the public can have confidence in the agency decision-making when it knows that transparency and accountability is built in.

Similar rules for the PCLOB, which is less public-facing in its work, but provides really important feedback to Congress and oversight over federal surveillance capacity. By removing PCOB commissioners, the Administration really undermined the ability of the agency, and therefore of the United States, to credibly commit to protect the data of foreign nationals or domestic citizens from government access. But that undermines our international relationships as well.

And I think the really important point here on removal is that people -- I sometimes hear people say, like, "Oh, yes, the president should be taking power for himself away from unelected bureaucrats." And I want to be clear that this is not a question of whether unelected bureaucrats, who, you know, Senate-confirmed though they may be, have power.

This is a question about the balance of power

between Congress, which set up these agencies and the laws it put in place to set them up, and the executive. And for the executive to unilaterally change that balance of power really undermines some of our most fundamental systems of checks and balances.

The president is also -- in addition to accruing power over government actors for himself, has worked to accrue power over private actors. We've seen him bullying law firms and universities, trying to control corporate speech via the FCC. We just had another example this week of Disney being asked to automatically or unusually reapply for all of its broadcasting licenses because of objections, again, to Jimmy Kimmel's coverage.

Even the FTC has been used in this space with a pursuit of a subpoena, basically a civil investigative demand directed at Media Matters, which was challenged by Media Matters in federal court, and the court, District Court, found that it'd -- it had been a retaliatory act in violation of the First Amendment targeting Media Matters' First Amendment exercise of its speech.

And I think we also have to note the fact that the President has extracted extraordinary contributions from private actors, both for his inauguration, which drew three times the previous record of million-dollar donors. Large, and the largest sector of donors were tech

companies who have extensive business before the federal government. There's also the Ballroom Project.

We think about things like the Melania documentary, the sort of levels of acquisition and solicitation of money explicitly and sometimes implicitly from private actors, tells us a lot about how that can be used to then coerce action or induce action from those actors.

So my argument is that when these things converge, the elimination of independence at agencies that were statutorily created to have independence, the accrual of executive power over private actors, then what you get is an architecture of coercion where dominant platforms become political allies, understanding that their economic futures are caught up in their relationship with the President.

This plays out in the privacy realm in two ways. First, you have this government as purchaser issue. When regulators are politically controlled, buying commercial surveillance data becomes much more permissibly allowable. They don't enforce the commercial -- the rules against that collection of data in the first instance, and then the government has more access to buy it. And when they can't buy it, they can coerce it.

And that allows the government to access detailed

behavioral profiles of basically anyone in the country, including their location history, their communications, their health decisions, their political associations, without a warrant, without judicial review, and without oversight.

Anthropic is a great example of this. It's not hypothetical at this point. When the Justice Department -- no, sorry, the Department of Defense was in contract negotiations with Anthropic, they wanted Anthropic, or Anthropic wanted explicit contractual protections against the use of its tools for two things: one, warfare, non-human involved warfare; and second, mass surveillance of the American people. And the Department of Defense resisted those terms.

When Anthropic declined to accept the terms, the Administration not only terminated its contract, which it certainly has the right to do, but it designated Anthropic as supply chain risk, threatening to bar any government contractor from doing business with it.

And that sends an enormous message to the rest of the private sector, "If you want to continue to operate, if you don't want to have a corporate death penalty, you're going to need to give us access to all of the data that you have." And if you're a company like Anthropic, you have astronomical amounts of data.

And I think it is notable that immediately after this contract dispute with Anthropic, OpenAI jumped right back in and made an agreement with the Department of Defense. Okay, so where does this leave us? Where does this leave you, importantly, in California and in other states?

States have an enormously important role to play. I talked a little bit about checks and balances at the federal level, but part of our federal system of checks and balances is the way the states can provide checks on the federal government and balance their actions.

Here are some things that I think are particularly important for states to think about. I have been railing against notice and consent models for data collection for a long time and advocating for data minimization models, and I would like to reiterate that advocacy in front of you today.

I think it's really important that we start going through substantive limitations on what companies can collect, how they can use what they collect, and how long they keep what they can collect. I think -- I think that when you put in place those mechanisms, it prohibits the strong-arming of data because you can't strong-arm data that doesn't exist to begin with. I think the minimization model in national security law is something

that we should think about a lot in commercial law, too.

I think it's also important that states enforce against commercial actors aggressively. If we can't trust federal enforcement because it's subject to political capture, we need our state AGs even more than ever. They can pursue data brokers, they can pursue surveillance practices, and they can pursue platform abuses.

CPPA has a great model, obviously, with independent expert analysis that's insulated from executive pressure. And I want to encourage coordination across state lines for national-scale actors.

And finally, I will tell you, I have always supported private rights of action, but the experience of the last couple of years has made me believe that they're more important than ever. We really can't depend exclusively on agency discretion, especially when it is subject to political control. Private enforcement can create a distributed accountability that cannot be turned off when executive control changes. So that's a particularly essential backstop when federal watchdogs are dismantled.

The stakes here are much broader than privacy. You care about privacy. I care about privacy. But I think it's important for all of us to remember that -- the reasons we care about privacy. And that is because when

unchecked surveillance power and unbalanced executive power converge, there is a threat to democratic participation, civil liberty, and human dignity. And with that, I am happy to take questions.

CHAIR URBAN: Thank you. Thank you very much for the bracing presentation. I'd like to acknowledge that Mr. Salgado also has a hard stop at 2:30. And so I want to be sure that to the extent we can, we can have a conversation with you all and also hear from him as well.

So I'd like to open it up to Board questions. And Mr. Salgado, how much time do you need for your presentation?

MR. SALGADO: Oh, this is for you. It can probably be 15 minutes, maybe even under that.

CHAIR URBAN: Okay. Could you think you could do 10? We're going to bargain.

MR. SALGADO: Absolutely. (Inaudible.) as little as long you want --

CHAIR URBAN: Okay. All right. Okay. So let's engage in some conversation at least until 2:15, and then we'll have a little bit of time for conversation with you too, Mr. Salgado. And if that's not enough time, then we'll figure out a mechanism by which we can all learn from you more. So questions, comments from board members for Commissioner Slaughter? Mr. Liebert.

MR. LIEBERT: Thank you so much, Commissioner, and I know I speak for a lot of people. Thank you for your courage, your truth-telling, speaking truth to power, and we really appreciate you taking the time to do this. I can't underscore that enough. And thank you to the staff and to the Chair for making this happen. I'm really excited about these informational hearings we're going to do now. We're learning so much.

My question would be, in this mutually reinforcing crisis in privacy protection, which you've alluded to, which do you see as the top problem? The opaque data broker market or the federal government's ability to buy and convert privately collected data into state surveillance without triggering Fourth Amendment scrutiny?

MS. SLAUGHTER: That's a very good and very hard question. It's like the inverse of when people ask me which of my four children is my favorite. Which of these crises is the worst is a little bit difficult to say.

I think they sort of have different solution mechanisms, which makes them a little bit different. I think that the warrantless access to commercial data that would not be acquirable with a warrant is a pretty profound problem. I know there are efforts underway to address it. I don't feel like they are moving with the

alacrity that they need to.

I think that the commercial data market problem is qualitatively different in some ways because its effects are much broader than just federal access. This is just one small part of it. I think it can have harms that extend much beyond that.

On the other hand, people also benefit from tools that are built off of data, right? I think AI tools have proven enormously valuable in many ways, and I think how you get that balance right is also a complicated question.

So I'm not sure that I would rank them in terms of priority, and I think that the solutions for them look a little bit different. So I don't think it has to be an exclusive action. I don't think -- I don't think it's mutually exclusive to pick one or the other to solve.

MR. LIEBERT: Thank you.

MS. SLAUGHTER: And some of the same solutions can apply to both.

CHAIR URBAN: Other board members? I wonder, Commissioner Slaughter, if there's any area in which you think states should not tread. I mean, there are obvious supremacy issues that all states have to be mindful of. But besides that.

MS. SLAUGHTER: I think the thing that I -- I think the thing that I worry about is less sort of

substantive areas where states should not go and more -- I do think we have to be mindful about the potential for conflict of laws between states. I do not think federal preemption is the solution, but I think that it is -- I'm sympathetic to the argument that it is meaningfully difficult for companies to comply when states have not only different but contrasting and incompatible requirements.

And so I think it's -- I would say, less about picking a subject area to stay away from or any sort of legal area to stay away from and making sure that there's harmony in the laws so that administrability is possible. Because at the end of the day, laws that cannot be administered because they cannot be adhered to are not going to be particularly effective.

And so thinking about what are the -- what are the ways you can put in place and work with your partners in other states to -- to create state sort of harmony between systems is really important. But I think this is a moment more than ever where states need to step up and show leadership.

I think it's important for your citizens, but I think it's also important for the rest of the citizens in the United States to see states doing that, and I'm encouraged that more and more of them are.

CHAIR URBAN: Wonderful, thank you very much. Mr. Liebert.

MR. LIEBERT: Data minimization seemed to be an area that you thought might be particularly rich for state action. Cut the spigot at the beginning and perhaps not as many Section 230 First Amendment-type issues, right?

MS. SLAUGHTER: Yes.

MR. LIEBERT: Is -- is -- is that a nice summary of -- of one of your clarion calls here?

MS. SLAUGHTER: Yeah. That's my -- that's sort of my core point, that I think we accept as a given a market in which all businesses are incentivized to collect as much data as possible, monetize it as much as possible, use it for whatever they can. And I don't think we need to accept that premise. I think that that may be how things have been operating, but it does not need to be how they continue to operate.

And when you think about solutions that fundamentally get to root causes, as I said, you can't access data that hasn't been collected to begin with. It cannot be breached. You know, whoever the bad actor you fear is, whether it's hackers or identity thieves, or governments, or foreign governments, which is another thing to worry about, they can't get what's not there to access.

And I think a lot of our rules around government access to data and warrant requirements are premised on the idea of sort of having to go case by case and person by person, you know, for example, to tap a phone, instead of understanding that single companies just keep all of this data on an ongoing basis now in a way that wasn't true when a lot of these laws were passed.

CHAIR URBAN: Thank you. Ms. Ozer.

MS. OZER: I just wanted to say that I very much appreciated your comments, and I am struck because I have been looking at some of the historical documents from the late 1960s and early 1970s. It's sort of the dawn of the computer age and sort of these deep conversations that happened at that point about real substantive protections and limiting actually collection and how data was collected and what data could be collected.

So I'm struck that what is old might need to be new again.

MS. SLAUGHTER: Yeah. I think it's a very astute point.

CHAIR URBAN: Thank you, Ms. Ozer. It's a disappointing point, but very astute. Mr. Mactaggart.

MR. MACTAGGART: Well, I just want to say, Commissioner, how much I agree with -- it's hard to come up with a question because I just find myself nodding the

whole time. I'd echo Drew, or Mr. Liebert, and say congratulations, and I'm proud of, as an American, of your courage. I hope your success successful.

And I'm always struck by, you know, here we have Congress turning themselves into knots over the FISA renewal, and meanwhile, these private entities know so much more about us and have so few -- you know, they have no restrictions essentially. So this was -- this kind of -- this vision was kind of why I got into this place in the first place, this space in the first place.

And people fault me for not having a private right of action, but it was important to get something. But I sure hope that the California legislature, you know, rectifies this going forward. We have this provision and it's gotten stronger. The law has and continues to get stronger.

And so I would just keep on saying to the California legislation -- legislature -- I hope you can make it stronger, so. But thank you for your time.

MS. SLAUGHTER: Can I just respond briefly? I actually have been very sympathetic in the past to laws that didn't include private rights of action. My perspective today is based on sort of new information and evolving facts and seeing patterns that I hadn't seen in the past.

And so, you know, I think it's important when you learn new things that you're open to changing your mind. And I think it's really important, especially in states, to be nimble in your adaptation to market developments and market changes. And when you try things that don't work or don't work as they're intended, to change them and make them work better. And that's actually exactly how government should be working. So I think I think it's a perfectly fine way to evolve one's thinking.

CHAIR URBAN: Thank you very much, Commissioner Slaughter. I echo all of my fellow board members' gratitude to you for your leadership. This is true leadership, and your example makes me realize that we don't see it as often as I would hope.

So I'll echo Mr. Mactaggart in saying I have pride in an American in your approach to these issues and in your courage in standing up for your -- the independent position of a Federal Trade Commissioner. We really very much appreciate your time today, especially as we know you have to go. And so we will send you away with those thanks and hopefully with some courage, further -- further courage, from California. Thank you.

MS. SLAUGHTER: Well, thank you very much. Thank you very much for having me. And thank you to all of you for your service and all of the speakers for being willing

to participate in this really important information-gathering exercise. It's really an honor to be included, and I'm happy to be available for any follow-up questions the Board has, by email or otherwise. I'm -- I'm -- I'm here as a resource.

CHAIR URBAN: Thank you so much. With that, we will move along to Mr. Richard Salgado, who's the principal member of the Salgado Strategies, LLC, and who is a lecturer at Stanford and Harvard Law School. He manages to balance both at the same time.

He has over 35 years of experience across the private sector, government, and academia, including as Google's Director of Law Enforcement and Information Security for 13 years, and as a prosecutor with the Computer Crime and Intellectual Property Section of the Justice Department.

And he has been kind enough to join us today to talk about access to data by the government through legal process and has been kind enough to be patient when we fixed our technical problems. So I will shut up, Mr. Salgado, and give you as much time as possible for what I know will be a very important and informative presentation.

MR. SALGADO: Well, thank you, Chairperson Urban, and it's an honor to be here. And if I can be useful in

any way, I'm very happy to do so. I'll probably skip slides given the time constraints here, and just focus on the major points I thought might be useful, and then -- some of which feed on what you just heard.

My -- my focus over the years has really been on security and on surveillance. An awful lot of the time has been spent with providers like Google and Yahoo. And to be sure, these companies have an awful lot of data, as do so many other companies out there, including app providers and others.

And Thankfully, we have statutes at the federal level and good statutes, like in California, better than there are at the federal level, that do at least provide some guidelines around government surveillance from collection of data and surveillance of these platforms, large and small. Most of the rules around the surveillance of and -- and capturing of data through providers goes back first to the Fourth Amendment, which is great.

We've got some constitutional rules and a baseline for what the government can do when it comes to search and seizure, as limited as that may be. But we also have statute. And in the United States, we have something called the Electronic Communications Privacy Act, and very -- more specifically to the kind of thing

we're talking about today, the Stored Communications Chapter of that statute. That really sets the rules of when the government can come in criminal cases to get the kind of data that you just heard about.

And there are really kind of three basic categories of data that Congress has set out and set around rules for government access to that data. The first is content of communications, which is probably pretty intuitive. It's the emails, it's the docs that you upload or create online, it's the photos that your phone -- you take a picture of a phone -- with your phone, it automatically uploads videos, that sort of thing. It's the content of what you want stored with the provider, maybe for later access, or sent to the provider so it'll send on to somebody else and you can receive stuff as well. That receives a lot of protection.

The next level is something called metadata or transactional data. That's information about the communications but not actually revealing what the communications say. So headers in an email, like who is the email from, who is it to, when was it sent, what was the IP address, that kind of metadata about the communication that doesn't reveal anything about the contents of it.

And then the last category is called basic

subscriber information, which is really the data you provide when you're creating an account with the provider -- your name, which might be fake, but it's your name, you might put an address, again, it might not be the real address, credit card information, probably real, might not be yours, but probably real credit card information. And that's stored -- and the IP address of when you created the account and the timestamp when you log in, that sort of thing. So sort of information about who the user might be listed out in the statute.

So those are the three -- that's how Congress back in 1986 defined the categories of user data and then applied kind of broad-brush rules for those categories. So it's clunky, but it has been administratable for these 40 years since -- since we've had the statute. But we are seeing serious creaks in this -- and cracks in this statute.

One of the areas, and this goes back to the presentation you just heard, has to do with the content that providers hold for users. It's no longer just the emails, and the photos, and the videos, but we are surrounded now by sensors, little devices that have sensors in them. Your phone -- you know, you think about your telephone, well, it's really a little black box full of sensors that show how fast you're going, what your

altitude is, maybe what the humidity is. It's full of things. It's hardly a phone any more and more of an environmental sensor.

And that data can be very useful. It can -- it can -- it can help drive products and make it know exactly where you are so you can get really good directions while you're walking or driving around. But it's you through your device uploading information about your environment. You might have a Fitbit or an Apple Watch that's keeping track of your heart rate, or blood pressure, or all sorts of biometrics, and uploading it to your private account for keeping, for you to be able to see your trends, maybe get a warning if something bad is happening, but certainly very private.

A carbon monoxide detector in your house, right? That's another sensor device that's keeping track of your environment on your behalf and uploading that data to a provider. And the reason I'm mentioning all of these things is that it certainly in my view, and I think the statute says this, those are all content.

It's your data that you're uploading, whether it's an email or it's the temperature in your house, it doesn't matter. It's your data in your account, and it should be protected the way all the other data in your account is protected.

But that's a philosophy that's somewhat at issue and -- and threatened a bit these days. There's this -- there's a case pending before the Supreme Court. We just had oral argument on it on the 27th of April, 2026, for those who might be looking at this later, called the Chatrie case.

And there, the question was whether the government has to follow the kind of Fourth Amendment content rules when it comes to a service where you are sending your location information from your device to an account so that you can later take a look at where you were.

And the Court is taking a look at whether a warrant is required for that, which is one of the highest levels of protection that we get in the United States from government surveillance, or whether that isn't required at all.

But probably more important, and this is what relates to the prior -- prior conversation, is the idea that perhaps the government can come to a provider who has a large swath of data and billions of users, and ask the provider, demand that the provider enter each one of the accounts of each of its users, each of those password-protected private accounts, looking for a particular piece of evidence. Whether that's permissible at all, and if it

is permissible, what level of legal process is required for it.

So that is a bit startling to and to me seems to be no different than if the government wanted to ask the Marriott Corporation to search through every hotel room looking for a particular weapon that was used in a crime, whether that is -- is really allowed at all or if it's a general search or not.

So that's the kind of question that is swirling around. It's being presented to the Supreme Court as a Fourth Amendment case. But that's exactly the kind of issue that really legislatures, state and federal, pretty well-suited to deal with. As long as they don't, you know, go below the constitutional protections, legislatures can deal with this better than a Supreme Court can. You can have the debates and the hearings and hear from a lot of people and not stuck on a single set of facts.

So that's one of the sort of hot issues in surveillance and talking about the pipeline of data from providers to the government. One that risks opening it up quite a bit into what -- what are often referred to as reverse searches, where you're looking through all the accounts looking for one particular person.

Another aspect that I think is -- that I think is

worthy of a lot of attention, it's been getting a lot of attention and justifiably so, is the idea that, you know, before we had the commercialized internet, and people really were relying on these online services for their day-to-day activities, if the government needed information, it needed your paper documents and your records, it would have to come to you for it.

It would have to serve a search warrant. Maybe it could use a subpoena. You'd have an opportunity to object. It would use a search warrant. It would kick your door in or come in, knock and come in, and get your papers. But whatever, you knew it was happening, whether it was through a service of a subpoena or the issuance of a search warrant, the inventory, all that, very likely you're going to know it happened.

Now that our private papers have migrated out of our steel cabinets at home and our mahogany desks and into the cloud, into the service providers' possession, these requests are not coming to us as individuals. They are going to the providers, and in huge amounts. This is a -- a common practice to go to the provider to get records rather than trying to go to the target or a witness to get them.

And really, there's no obligation for the government to give notice to the user that this is

happening. So providers have tried to fill that gap and have adopted policies, and this is really almost universally true, I'm sure there's examples where it's not, but where the provider says, "When we get a demand from the government for your user data, user, we will let you know that it's happening, unless, of course, we're gagged, unless there's a legal prohibition against the disclosure."

Unfortunately, that is exactly what's happening. In the majority of cases, when a provider gets a piece of legal process for a subscriber, it also comes with a gag order from the government. It has become a routinized practice. I think Meta, in its last disclosure on this, said it was something like 77% of the orders they get come with these gag orders. That's very high.

You know, the secret searches of this nature were really meant to be the exception, not the rule, and that's been flipped on its head. So that's another thing that really needs to be addressed. Again, it could be done by a court if the court were to find that one of the Fourth Amendment requirements is notice, and there's a good argument for that.

But really, this is better for legislatures, rulemakers who can say, "Look, you got to give notice, government, or at least let the provider give notice,

unless there's some really extreme exceptional circumstances that make giving notice to the user a problem." And there may be, there's -- there's lots of situations where that might be the -- the case, but it's not 77% of the -- of instances where courts are issuing these orders.

So, yeah, that's the second sort of hotspot. In addition to these -- try to rein in these, the potential anyway, for a large number of reverse searches where all our accounts are searched looking for evidence, and the notice issue so that we can at least know when it's happening so we can assert our privileges and other objections to the disclosure before it happens.

Those are the two areas that are very obvious for Congress to update the statute. Like I said, it's a 40-year-old statute. Congress thought it would only last seven years or maybe ten years. This was in 1986. It hasn't been meaningfully updated at all, and so 40 years later, it's not surprising that the statute has shown serious cracks.

I think I've already gone over the ten minutes you gave to me, so I'll --

CHAIR URBAN: Thank you. Yeah. We're also running up against your stop. Do you have a few minutes for questions? Okay, great. Thank you. Do we have

questions, Ms. Ozer? And then Mr. Liebert.

Oh, okay. Mr. Liebert, please go ahead.

MR. LIEBERT: Thank you so much. That was, again, very illuminating. In fact, the last thing you pointed out is fascinating, this idea about states somehow banning or regulating, if you will, this notice issue to protect their -- their members from these types of secret searches.

And I'm wondering, have any states that you're aware of attempted to do this? And I would assume then the federal government would seek to have those -- those statutes invalidated, or would California be the first to do so, at least to attempt to do so?

MR. SALGADO: No. States can do this. It would only be applicable, of course, to state legal process. It wouldn't work to -- to regulate the legal process of other states except where the order needed to be domesticated in California, and it wouldn't be effective against the US government, but it would be effective against or as to the state authorities.

And it would unlikely be a ban, it would likely be that a higher showing, an actual need, is demonstrated by law enforcement, a very fact-specific to that case, why can't you tell the user? Does the user not already know about the case? Is the user the suspect or is the user a

witness? Like, really getting into the facts rather than it just being a boilerplate rubber-stamping.

MR. LIEBERT: But our bigger problem is -- is the fact that it's actually the federal government that's engaged in this practice, right? So that we're not so much afraid of the state here in California doing this practice as we are the feds going to the providers saying, "Secretly hand over the -- the information."

MR. SALGADO: That's right. And, you know, there is a federal statute that's a federal bill, I should say, at the federal level that is shown to be pretty popular. It passed the House, I think, unanimously twice. It's called the NDO Fairness Act. It has a good shot, I think, if we can get a vote on it in the Senate. And having states chime in on it, I suppose, could be -- could be useful.

And that would actually be nationwide and could affect state legal process as well. So it needs to be -- it needs to be at the federal level to really have effective, you know, use, not just at the federal, but across states as well. But there is a vehicle, and it's sitting there ready to go, but it does require Congress to act.

CHAIR URBAN: I'm just pausing on that. Ms. Ozer, please.

MS. OZER: Thank you so much for being here, Mr. Salgado. You -- you discussed the 1986 Electronic Communications Privacy Act. I just wondered, you know, here in California we have a more modern law, the California Electronic Communications Privacy Act of 2015. And I wondered if there is, you know, how well is that faring? Are there sort of additional provisions that might be -- need to be augmented given that it's now been 10 years?

MR. SALGADO: Yeah, that's right. And the CalECPA was a model when it was passed for updating legislation, and it would have been great if the -- the feds could follow what California did. I think it is -- there is some room for improving CalECPA.

One of the ways would be around what I was referring to earlier, those reverse searches. A -- a large proportion of the reverse searches that Google was receiving that were of the nature in the Chatrie case, their so-called geofence warrants, a large number of those came from California. So it is clear that reverse search technique is being used by California authorities.

Updating CalECPA to better deal with those kinds of searches, I think it depends on what Chatrie -- what the Court says in Chatrie, but given the situation as it is right now, that would be a good area for improvement.

MS. OZER: And just one additional follow-up. Sort of -- you know, given sort of the advances and sort of the increasing use of artificial intelligence systems, is there sort of any additional sort of holes or needs you see? And -- and I have -- I think you recently might have written something about sort of AI issues, and -- and demands, and reverse searches, so I just thought maybe you could share a little bit of -- of how this is intersecting with increases in use of AI systems as well.

MR. SALGADO: Yeah. I mean, AI is going to end up everywhere. It's going to end up with the government using it to identify targets. It can be used with -- to run across the data that's been produced to the government or that the government's purchased and all the other points where the government's able to obtain and collect data. And from that generate targets that they can conduct further surveillance on. That's a whole issue set.

What probably -- the one -- this may be a little fanciful at this point, but I'm not sure how fanciful it is. It would be, you know, in the future here, but it would be where the government uses what is essentially a reverse search-like theory, goes to a provider and says, you need to run across your corpus of data using some AI-searching techniques, right?

Not based on fields in a database, not based on a target identifier, but sort of the logic of the AI to reveal the information you have about a particular class of users, maybe one user, maybe an entire group of users. So there -- there -- that -- that is a form of a reverse search that you could imagine an aggressive government entity wanting to pursue, combined with -- and you'll be familiar with this -- but combined with a claim that you can compel the provider to give assistance for the search, which is necessary for all of these things.

It just starts pushing an awful lot of the analysis to the provider to do, and the use of AI could augment that. And that has really been the trend over the last -- if there -- if there -- of the many trends over the last 30 years, it's been to -- for the government to push more and more of the analysis work to the provider to find the information and produce it, rather than the other way around where the information is produced and then the government analyzes it. And AI could put that on steroids.

CHAIR URBAN: Thank you, Mr. Salgado. Additional questions from the Board? In that case, I will thank you for your grace under tech fire and patience with us and that very informative presentation about how the government is acting under legal process and some of the

challenges that arise there as well, and leave you to picking up your kids or whatever it is you have to do here at 2:30. So thank you very much, Mr. Salgado.

MR. SALGADO: Thank you.

CHAIR URBAN: We will now turn to a more technical discussion to help the Board and the public understand some of the data flows that we've been talking about from the perspective of those who are thinking about them from a technical perspective.

We turn to Dr. Nathan Good, who is founder and CEO of Good Research, and Jennifer Chen, who's the Head of Operations for Good Research. Dr. Good earned his PhD from UC Berkeley School of Information, and his company works with organizations to assess and manage digital risk across apps, websites, AI systems, and data sharing ecosystems.

Ms. Chen oversees product and operations for Good Research Privacy and Technical Investigation work, and they will be presenting on consumer data flows in the mobile ad marketplace and the potential for tributaries of data to flow in unexpected ways.

And with that, I will turn it over to you, Dr. Good and Ms. Chen. Thank you very much.

MR. GOOD: Thank you. Thank you all for having us. Can you hear me all right? Perfect. So this will be

a bit of a change of pace from the previous presentations. I'm not going to be talking about legal frameworks like CCPA or GDPR. We're going to get pretty nerdy, or as nerdy as we can get in 15 minutes with no code.

But it's a -- it's a real honor to be here today and to talk about this -- this ecosystem and to be able to share our -- our sort of view on it and what we've seen, and what we can teach both yourselves and the public. Really looking forward to the types of questions you have and to -- to walk through it. So you go to the next slide, please.

So just -- there we go, it's directional. Awesome. So just really quickly to give you a quick roadmap, I'm going to talk about some pieces of this ecosystem that are important to understand as we're talking about data flows and data that's being collected. Then I'm going to talk about some of the key risk points that we see in this ecosystem and the way that these manifest in the data flows.

And then, you know, the example, the Kochava example, Commissioner Slaughter did a pretty good job of talking about that. So I'll probably spend a lot of time on the first two because there's a lot to get through. So if you can get to the next slide.

Yeah. So this is complicated on purpose. This

is a -- actually a simplified version of the ecosystem that we all live in today. And I'm not going to take the next 15 minutes to walk you through all of it because that would be painful for everyone here.

But the idea here really is to communicate the degree of sophistication that this ecosystem has and the way that data changes hands across lots different parties in the ecosystem, and the way that each one of these exchanges constitutes agreements. And they constitute ways that people have expectations that are being set, and that ways that data is being allocated for sharing or purpose for sharing. And this happens throughout the entire ecosystem.

And so when we talk about the words data sharing and transferring data between entities, we're talking about a lot of hands. We're talking about a lot of different ways that data can be collected and shared.

And so what I'd like to do is talk about the main components of this just to make it easier to understand at a high level what we're kind of talking about when we're talking about data collection and data sharing.

So there's -- I'm vastly oversimplifying this, but I'm going to be focusing most of my conversation today talking about apps, SDKs, and data brokers. And so an app can be a web app or a mobile app. I'll be focusing today

mostly on mobile applications because of the points that were made in the earlier presentations about the data collection capabilities that these devices have.

An app is essentially just software that runs on your phone that can communicate with the various different functionalities that your phone has; collect information, and perform some sort of function that the software developer intended.

What's really interesting about apps that I think the public and maybe a lot of people don't necessarily know is that an app largely consists of other code. And so in an app, you may own the idea of it, you may own the responsibility of it, but most of the code that builds your app is not really your own. It comes from third-party SDKs, or from other -- what we call toolkits, things that you're using.

And what is an SDK? An SDK is code that somebody has made for you that's called a Software Development Kit. And you can think of them -- the way that I like to describe it is is -- is Legos. You're grabbing all these different Legos, you're putting it together, and that's what makes an application.

And a software development kit, the reason why you do this is because people have gone through the work of putting together some tools that you can use. And so

you can pull all these different things together and you can stack them and glue them together using code, and you can build the functionality that you have for your app at a fraction of the time, effort that would require to do it all on your own. So SDKs are consequently incredibly popular, very fast ways to build an application and are pervasive throughout the way that modern software development works.

Then we talk about data brokers, and I'll be talking about this a bit more, but data brokers come way down the line when data has already been collected and -- and sold, and transferred in different ways. And data brokers have -- are a very different part of the ecosystem as opposed to in the very beginning.

So data brokers are taking this data and monetizing this data through licensing and other different means. But all of these are connected through this ecosystem that I'll go into shortly. Next slide, please.

So one thing that I think is really important to understand is when we talk about collecting information, and the previous presentation mentioned this as well, that these mobile devices that we carry are very intimate devices that contain a lot of different capabilities. And -- and they're not -- they're called mobile phones, but they're much, much more than that nowadays.

And these mobile devices, they contain these various different sensors. And one bit of sensitive information that comes up and is discussed quite a bit is the idea of location information. And I'd like to just take a little bit of time, and not enough that we'll go through every single part of this diagram, because it's somewhat overwhelming on purpose, is that location information is not just the GPS coordinates of where you are.

Location information can be derived, it can be inferred, it can be created from lots of other different what we call signals or indicators. And -- and I think it's really important to understand that when we talk about data about a person or about an entity, we're not talking about a single piece of data. We're talking about lots of different types of data that can be combined to give you an idea of that person, or that feature, or that relationship.

So location is a great example because there's many, many different ways that you can determine location. So, for example, I'm sitting here in this room and I have my mobile phone with me. My mobile phone is trying to connect to Wi-Fi even though I really don't want it to, and when it's doing this, it's saying, "Hey, I'm this device and I'm trying to connect to these Wi-Fi

locations."

And these Wi-Fi locations, they have a certain signal strength attached to them, they have different bits of metadata, as we heard in the previous conversation, and all of that information helps to create sort of a graph of the world that we live in today, and so that's called Wi-Fi positioning.

And so just without any GPS, you can sort of kind of know where people are based off of the Wi-Fi locations that are around. You can do this similar for cell tower signal strength, and then you can combine these bits of information in order to get assisted levels of fidelity.

So GPS, for example, doesn't work really great in a building, but if we combine it with Wi-Fi strength, for example, then we can have an assisted GPS, which now we're saying, okay, now we have a better idea of -- of where you actually are at.

And so I make this point to basically give everyone sort of the understanding that location is not just one item. Location is combined factors that you can use to get precise understanding of where people are. And this is one type of information that's very sensitive that we talk about a lot when we're talking about personal data, and it's also incredibly complex.

So I want to go to the next slide. And so I took

a portion of that very, very complicated graph that I showed you earlier, and I flattened it out a bit to make it so you can kind of see how data can traverse from left to right. And I want to take a little bit of time to walk through what -- what you're looking at right here, and all the pretty little lines are connecting all the little boxes. They all mean something.

So when we look at the far left of this, that's the mobile application that we were talking about earlier, and that mobile application is -- consists of all these different SDKs, and these SDKs are reflected to the right of that. And these SDKs take data and lots of different types of data potentially, and they store this information for use in many, many different types of functions.

And the one thing I'd like to sort of point out is that the SDKs can have single functions, they can have multiple functions, it really depends on the sophistication, and you can configure them in different ways. So you can have an SDK that, for example, listed here, that is a crash reporting SDK, but you can also have other functionality built into it too, and that depends on the developer, the defaults, things of this nature.

So as you're collecting this information from the SDKs and it's stored in these databases, then you have the ability to do something with this data. And to do

something with this data can be many different things. It could be enhancing the functionality of the services that you have, could be using it for monetization, you could be selling it down the line. And in the case that data is being sold and used, that's where your data brokers come in.

And so data brokers have the ability to buy data from lots of different people who are selling it, and then, you know, selling it to customers. And I want to kind of focus on that part for a little bit because I want to make sure that people are not making the assumption that data brokers are only getting data from a single source.

So you can get data from multiple different sources, and this is really interesting because when you combine data from lots of different sources, you can take disparate data sources and you can make inferences as we talked about before. It also can remove -- so the people at the very beginning, for the mobile apps, for example, they may not even know at all -- in many cases they don't -- what's going to -- happening downstream.

And so as you move further and further downstream, there's less ability for the people at the collection, for example, to understand how the data is actually being used. And -- and I think that's an

important thing to know because we don't really have good technical means of saying this data is specifically for this purpose. Once data starts to make its way into an ecosystem, that data can be used in lots of different ways, and there's not really a way for the people who collected the data to know how that's being used. That's in these various different exchanges that we see as it moves through the ecosystem.

And then finally, you have the customers, and the customers don't have to necessarily buy data from one data broker, customers can buy data from multiple brokers. And so even in the case that one data broker may have only a bit of information, a customer would say, "Oh, well, if I go to these other data sources, I can use this information, I can combine it together."

And so when you look at the complexity of these various different parts of the ecosystem, there's lots of different ways that people could combine this information to reveal personal information or to circumvent maybe even protections that that happened at the front.

So I'm going to go a little bit into the risk points and try to make it on time. So there's -- people make mistakes. The internet is filled with boo-boos, and there's a lot of misalignments and misunderstandings as people are pulling together these complicated apps in

these ecosystems. And as we talked earlier about SDKs, for example, some SDKs can be very complicated. The way that they can be implemented can be changed.

And so you can have issues like data leakage that happen purely through problems that people don't understand and misunderstandings that happen. And that's very, very common as you're working in these ecosystems. And misunderstandings can happen in lots of different ways. There can be a misalignment. For -- for example, you're using an SDK that you shouldn't be using for, say, children, and the developer may not know that, or the developer may not know that this data transfers to a different location in the world, things of this nature.

So you can have those types of misalignments. You're using the wrong tool for the -- for the wrong purpose.

You can also have misunderstandings where you have, okay, we're configuring it a certain way, and we thought it did these things, but it actually doesn't. It seems to be doing something else.

And all of this can result in additional data being collected that isn't supposed to. You can also have a lot of problems potentially with data leakage when these things are not aligned properly.

And then lastly, there's this issue -- when I was

talking about combining datasets -- of what we call bridging. So if you could go to the very last slide. So bridging is the least complicated slide here, so -- but it's also one of the most complicated topics that we have. So I tried to make it really sort of simple here. But bridging essentially allows you to connect a -- a persistent state of a person.

So in the ad space, we have identifiers that are tied to your -- your device has a unique identifier. Person, you know, on this device, if you're connected to this device, you give it your information, that's sort of connected to an identifier. And there's ways that are -- are much more unique and tied to a persistent identity of yourself, and so we call those persistent identifiers.

And then there's what's called ephemeral identifiers, and these identifiers, they change over time. Some of these are as a result of things you can do on your phone to preserve your privacy. So you can change specific identifiers. Some of these are just time-bound, they're session-based.

But when you connect these two -- so if you use something for an ephemeral case, and -- but you're able to connect it to a persistent identifier, you're able to bridge this personal information that maybe was not related to an actual person to an actual person. And this

bridging behavior is something that we see is -- can be problematic in this space.

And one of the key points of issues that you have when you're trying to protect users' data down that down -- as you're moving it downstream, all that takes is one ability to bridge these identifiers, and then all of those protections can go away.

And so I think I'm at time, so I'll hand it back to you all and so we can try to --

CHAIR URBAN: Thank you. Thank you very much, Dr. Good. That was incredibly informative and also sobering. I guess I'll kick us off with a question about a theme that I'm not going to ask you to do legal analysis, but a theme that we've been hearing from prior speakers goes back to data minimization, meaning, just don't collect the data.

I thought I heard you saying that when you're building something from the building blocks of SDKs, sometimes you don't have full understanding of how those are going to behave, and even if you do, you don't have full understanding of how things will behave down the chain. First of all, so I guess my question is, is that correct? And secondly, what does that mean for data minimization? And if you have any thoughts about what that means for us, I think we'd be grateful to hear them.

MR. GOOD: Yeah, for sure. I think it is definitely the case that you can have SDKs that you don't necessarily know everything that they're doing, and that data can be collected for a variety of reasons. And I think from a data minimization perspective, this makes it challenging and it sort of begs the question of how -- how -- how do you actually know that it's doing what it needs to?

And so there's -- there's a lot of ways that developers and different people can communicate. There's like different agreements that you can have in place, but there's also just checking, I think, is really sort of important.

Because, as I sort of mentioned earlier, certain SDKs can have multiple purposes associated with them. And so if, for example, you're using the SDK only for crash analytics, you want to make sure that it's only being used for that purpose. And it might have additional settings that you're not aware of.

So I think data minimization, from my perspective, is a -- is a level of diligence that's required. And -- and also communication, because as we see sometimes, the -- the capabilities of an SDK aren't necessarily as well communicated as they could be, and so there's misunderstandings there that could impact data

minimization.

CHAIR URBAN: Thank you. And just as a quick follow-up to -- to -- to just push on it a little bit, so the kinds of steps that somebody who wants to use an SDK should follow, do you have examples that you would suggest?

MR. GOOD: Absolutely. I think in most cases when you're using an SDK, an SDK should have some sort of data processing agreement or something in place. You're going to want to definitely look at that.

You're going to want to understand the -- the functionality. You're going to want to check to make sure that you're implementing it properly, and you're also going to want to make sure that the use case for that SDK matches the use case that you have in alliance with the purposes that the SDK both says it should be used for, as well as the -- the app itself.

CHAIR URBAN: Thank you. Ms. Ozer.

MS. OZER: Thank you, Dr. Good. I wanted to just have a little bit more of a sense of sort of the ecosystem of the SDK developers. So what are the business models of these SDK developers? Are they selling the SDK for money, or do they still retain some access in terms of the information that's collected with the apps that are using their SDK?

So like, who are these people and what is their business model?

MR. GOOD: Yeah. That's a -- the answer is everything. I mean, an SDK can be very, very broad in the sense that you have SDKs that provide everything from analytics, to fraud protection, to understanding whether or not there's been technical issues with the application.

And so in the business models around them, they vary from, you know, you pay a fee to be able to use an SDK to provide information for you or to provide a certain functionality, to, you know, they let you use it and they -- they have, you know, that data and they use that data for -- for monetization purposes.

So it can -- it can -- it can vary quite a bit. You know, SDKs are essentially tools and functions that you'll put into your app to provide certain functionality that you need.

MS. OZER: So there may be developers using SDKs, and those SDKs are actually accessing information in the apps that are built by those developers, but -- and how much transparency is there in terms of the final individual sort of knowing that?

MR. GOOD: Yeah. That's -- I mean, that's definitely been a challenge in this space because the -- there are certainly the things that an SDK will say and

what a developer expects. So there's the sort of public-facing agreements, there's the documentation and things of that nature. And in most cases, that probably works pretty okay.

But then there's also the actual implementation of it, and then that implementation, you really want to be able to look and see what that SDK is doing, because there have been many cases where developers have been surprised by what an SDK is collecting and what that information is.

And that -- you know, that's unfortunately, it's work. It's -- it's not straightforward all the time to be able to do that, to be able to -- to go through and check it out. But if you do sort of want to understand that, I mean, there's certainly conversations you can have with SDK developers to understand that, but also just checking to make sure that the data you're providing is in line with the data that you expect to be collected.

CHAIR URBAN: Thank you. Mr. Liebert.

MR. LIEBERT: Thank you so much, Dr. Good. Once again, another amazing presentation. And one of the things that shocks me about your presentation with all those charts is I need to know why you haven't become a Luddite, because you know too much, right?

And so one of the things that I want to ask you about in that regard is, as we focus on the data

minimization issue, it seems like one of the implications of -- of what you're pointing out with these amazing charts of the sharing and selling of this information going all the way through all of this sifting, is it even literally possible without massive enforcement divisions to be able -- to oversee alleged commitments that are being made about the protection of this data?

MR. GOOD: Yeah. I think that's a -- it's a fascinating question. And I -- as I kind of mentioned earlier, there's -- individual commitments are being made between individual actors as they're passing this data back and forth. And I think that's an area where there's a lot of promise, right? Because effectively, you know, to the -- Ms. Ozer was asking earlier, how do -- how do people know what's going on? That's a fundamental brick of commerce is trust.

And trust between people who are exchanging information is the backbone of how we do business and how we do commerce. And all of these individual decisions are being made. There's agreements and there's an understanding of what's going on. And that's -- that's the potential, I think, to really do this.

I think you're absolutely right, the idea that somebody could come and monitor the entire ecosystem, that's -- that's unrealistic. But I think, you know, with

the right incentives in place and, you know, people don't want to be screwed over, for lack of a better word. They want to make sure that what they're doing is in line with their expectations.

So each one of those agreements, I mean, for thousands of years in human commerce, we've -- we've dealt with this problem of how do we make sure that we're agreeing to the same thing, and that fundamental notion of trust is incredibly important to this ecosystem to work properly.

CHAIR URBAN: Ms. Hamer.

MS. HAMER: Yeah. Great presentation, by the way. Thank you. So I'm interested in the bridging, the ephemeral -- those IDs with the persistent ones. So it sounds like it pretty much throws not just data minimization but purpose limitation out the window, and the enforcement issue. So the people on the front end of the app think they're doing the right thing, but as the data flows through the ecosystem, they have no way of knowing.

So from a regulatory standpoint, you know, what do you suggest?

MR. GOOD: Yeah. Oh darn, I'm not a lawyer. But I think from a --

MS. HAMER: Just from a data mapping standpoint.

MR. GOOD: Yeah. I think from a data mapping standpoint, I think, again, those -- those connection points between those graphs are -- are incredibly important. And making sure that those connection points between data exchanges are in line with the expectations really, really matters a lot.

And so, for example, if you're collecting location information and you're doing a really good job of minimizing this, this and in the context of, I don't know, some -- some sensitive use case, then -- then making sure that that data is contained in that use case is going to be very, very important.

Where the types of bridging information issues start to happen is when it starts to kind of escape from those boxes. And -- and sometimes escaping is deliberate, sometimes it's just somebody thought they had a really good idea, and they don't sort of consider the -- the other consequences to it. And I think those are the areas that you can kind of focus on, of making sure that people understand that when you're doing these exchanges, to really be cognizant of the -- the -- the limitations of that collection use case.

MS. HAMER: Right. The unintended consequences are the ones --

MR. GOOD: Exactly. Exactly.

MS. HAMER: Thank you.

CHAIR URBAN: Additional questions? One -- many, yes. We might need to follow up.

MR. GOOD: Please do.

CHAIR URBAN: Yes. Thank you very much, the team from Good Research. I know that you know a lot about this and many people do not, so we really appreciate you taking the time to come and give us this insight into the data flows, as difficult as it may seem to map some of our theories and policies onto them. It's -- it's been very helpful. So thank you very much.

MR. GOOD: You're welcome.

CHAIR URBAN: And with that -- with that, we will move to the third stage of presentations. I'm going to ask the folks on this panel to try to keep your remarks to 10 or 15 minutes if you can, and then we will engage all of you in conversation.

Our speakers, our topic for this panel is broadly speaking policy approaches to the federal use of commercial data. And our speakers include: Jacob Snow, who's a Senior Staff Attorney with the ACLU of Northern California; Madeline Dwyer and Tom Bowman are presenting from the Center for Democracy and Technology; and David LeDuc, who's the Vice President of Public Policy for the Network Advertising Initiative. Welcome to all of you.

Thank you very much for taking the time to join us.

And for those of you on the East Coast, I know it's getting into the evening, so we especially appreciate it. Mr. Snow will kick us off, and I believe has some slides.

MR. SNOW: Good afternoon. Thanks. It is an honor to be here to present to all of you. It's also an honor to be on this panel with the amazing experts. All of the -- the -- the talks so far have been fantastic, and I've learned a lot. So it's just a wonderful thing to be here. I -- there we go.

I'm going to talk about three things today. A lot of what I had planned to talk about is a little bit duplicative of what other folks had said, and so I will go through that more quickly and then we'll have more time for -- for questions. And then I'll add some other things as well.

But in general, I want to talk quickly about the kind of foundational question of what our locations reveal about us, and then how governments and companies are tracking that information, often in secret. And then third, some of the policy approaches that we might think about to address it.

And my remarks today will be a little bit more, I hope, able to give like a real-world impact to some of the

more abstract things we've seen already. I found Dr. Good's diagrams to be incredibly illuminating and helpful, but I will talk about things in the real world and how they impact people, and I do think that pairing hopefully will be powerful.

But in terms of the scale, we do have hundreds of millions of mobile devices being tracked through all these mechanisms that Dr. Good and others have described, and that results in billions of location data points. And that's not billions of location data points overall, it's billions daily. It's an immense amount of location information that's collected about people as they move about their communities.

And I want to think about what our locations reveal. And I wanted to talk about this from my own perspective. As I was -- as I've been thinking about how to communicate the privacy harms of location information, I used my phone my phone to collect my own locations for over -- for nearly a year. And as part of that work, we worked with a data science master's student, Brandon Miner, from the University of San Francisco, to analyze my location information.

And my plan was to try to present some of that location information in a way that would explain the intrusive and invasive quantities -- qualities of that

location information. Unfortunately, after doing that analysis, I found that it was not safe for me to do that in this public setting.

I tracked my -- I live in San Francisco, and I tracked my own locations all around the city, and it showed my home; it showed the place where I work; it showed -- that says client meeting, but it's a little bit hard to read; it showed my trips with my children to a public library on the weekend; it showed my close friend's home that I visit regularly; showed the location of my children's elementary school; the route that I take to take them to that elementary school; the place of the soccer games on the weekends where I go often on Saturday with my family; as well as political protests; and other medical, dental, a trip to the ER one night; like, all of that information was revealed in my locations.

And this map does not show those actual locations.

CHAIR URBAN: I was going to say, what's the unsafe information --

MR. SNOW: Like, what are you doing? Why are you doing this? Yeah. So these are not the actual places where those things happened, but they were revealed to me in that data set. And so from that, you have the location points, the fields, as Dr. Good described them, but then

you can also extract inferences from them about places I've been, what I've done. And of course, from Commissioner Slaughter's discussion, all that information is actually being generated.

And from the work that we did with the data science master's student, I can say that it is not -- does not take an immense amount of resources or technical ability to do this. Like, have a brilliant master's student working with us, but it's just one person in a master's program who's able to do it and pull out all these inferences from my data.

And what are the impacts on people from gathering all of that information? The impact is the human cost that we see in our eyes in a society where armed agents are roving our streets and they are capturing people and they are separating families.

So this is Liam Ramos, the boy who was captured by ICE in Minneapolis. In this horrifying picture, It shows him being detained on his way home from school. And the consequences of surveillance of all, of those locations stored in all of those databases in abstract columns in Dr. Good's slides, land in the real world in stories like this, where people are stopped on the street and they are incarcerated, they're detained, and they are taken away from their families.

And so as we think about the impact of privacy law, we need to keep in mind that it harms real people in the real world, and we have to ask ourselves if we're okay with that. And we've seen it in Minnesota, but we've also seen it in San Diego, where there's an ICE arrest at a school last year.

And the consequences of that are not just that a single person was separated from their families. In the wake of those kinds of abductions, people become concerned about going to work. They could become concerned about going to school. And there are ripple effects for the education and learning of children when we have a surveillance apparatus that allows these kind of events to become pervasive.

So now I want to talk about how commercial surveillance becomes government surveillance. A lot of this is stuff that has already been covered. There is a billion-dollar market in people's locations, and this is built out of the fact that in modern life, all of the devices that we have around us on our persons, and our homes, and our cars, they are all in one way or another covertly monitoring us.

And that includes, you know, cameras, televisions, entertainment centers, our cars, the tires on our cars, for Christ's sake, and they are being covertly

monitored and -- and often used to generate profiles of people. It comes from cell site location information as we just use our phones to go about the world; apps collect it, and this is also illustrated so concretely in Dr. Good's slides.

We see this in our apps that we but we don't maybe think as much about the impact when that information is being packaged up and sold to the government. And the impact of that is examples like this, where a Muslim prayer app was used to generate and collect location information about people who used it.

And to me, there's a few things to lift up about that story. One is that, from what we know, that was an SDK that Dr. Good talked about that was installed in not just that app, but also in many other apps that collected people's locations.

And Board Member Ozer asked about the business model of some of these SDK companies. In this instance, I think the business model was that the SDK company was paying the app because it's hard to run an operating business, for example, with a service like a prayer app or something that people might just want to use on a daily basis, but they can't afford to pay a lot for. The SDK company was paying the app vendor to install the SDK and then collect that information. And so in that sense,

buying data from these apps.

So those SDK companies are data brokers, and they both buy the data from -- from an app by asking to install the SDK, and then they sell it to the government. The -- the impact of this, by the way, is that you end up with disproportionate targeting of marginalized communities based, frankly, on anti-Muslim bigotry, where the government wants to collect this information and track the locations of people based on their religious beliefs arising out of pure bigotry on the part of the government.

We see it also from web browsers, but also from real-world surveillance, where ALPR companies like Flock have pervasive monitoring apparatuses in cities, and then they use that surveillance data to build, like, a people -- a people lookup tool, as 404 reported.

Also, in the real world, when you go to a retail store, you might be recognized with facial recognition. That could associate you with either your identity, you know, a picture that they have from some other source, or it could just identify you across visits to a retail store. And then you might have to -- then there might be some bridging that happens to connect that to a real identity. But that real-world surveillance also becomes location information that can be shared with the government.

Finally, as we've heard about today, it comes from the advertising marketplace and the behavioral advertising marketplace as well through the -- the systems that we've heard discussed in Dr. Good's and other presentations.

One thing that -- that I would like to add to the set of diagrams for the Board to look at is this one from a report called America's Hidden Security Crisis, which talks in actually a little bit less detail than Dr. Good's diagrams. And it just shows how all this information is broadcast across an enormous network of entities. And this is, to be clear, to serve a single ad.

You go to The New York Times, you go to a website, you look at your phone and an app, and you see a single ad, and all of these data flows, these transmissions of information, are a result of the bidding process to give a single person a single ad in a single moment on a single day.

And you might hear that the information that is transmitted in those systems operates on a pseudonymous or anonymous way. And this gets to the bridging idea that Dr. Good talked about, and -- and also the notion that Board Member Hamer asked about with how do we address this bridging in a regulatory framework?

And the one thing that I would add to that is

that this bridging and the sort of pretending like the bridging doesn't exist is a way to categorize data in certain ways that matter to the law. So the CCPA, of course, has this category of sensitive information versus non-sensitive information; it has precise versus non-precise geolocation information. Other privacy laws have this notion of personally identifiable information, which is associated with a person.

And if that bridging allows data flows to happen where it pushes it outside of a certain category under the law, then those flows can happen uninterrupted. And then on the other end, they can be reassembled so that the flows happen, but the legal accountability and the legal restrictions that do exist under the law are evaded. And so, I think bridging is a really important thing to keep in mind when we're looking at how data is categorized under privacy laws.

And of course, as we've heard, the federal government is buying this information. They're using it in immigration enforcement. There are lots of stories. I mean, just recently, like, in March, the FBI director confirmed that they are buying location information and that they aren't -- they're not going to stop. Senator Wyden and other Democrats called, of course, for an investigation into these purchases of data.

And so where we are for location surveillance is that we have few effective limits; it's a valuable mechanism of surveillance; and it's especially dangerous in the world that we live in today, where it is held by a violent and repressive authoritarian government of our own.

So to talk about a few policy approaches -- I will add my voice to those calling for strong data minimization. I would say that it should be paired with opt-in as -- as a baseline along with strong data minimization. And I do think that looking at it from that perspective all the way down at the collection level is one of the most powerful ways to stop this because, of course, once data is collected and is in possession, it's much harder to limit whether it is shared, and also it can be accessed through compulsory means with warrants or other kinds of subpoenas, including administrative subpoenas, which we've seen abused recently.

I also want to talk quickly about notice and what notice does when we all encounter it in the world. This is a variety of notice. There's a dangerous cliff. A sign says, "It's unstable. Warning. Stay away. Don't go on the cliff."

Now, this is another kind of notice. A sign saying, "If you approach the cliff, you agree to our cliff

policy." That cliff policy could say, "By the way, approaching cliffs can sometimes result in a sudden increase in the acceleration of a falling body. Though that acceleration can be -- sometimes be harmful to humans. Take that into -- all into account as you make your decisions in your life. If you have a problem, you're going to -- you're going to forced arbitration, by the way."

So if you think about those -- these two different kinds of notice, two things to lift up. One is that transparency alone cannot avoid making judgments about what privacy and safety mean for people. A privacy law can't just say you have to tell people. It sometimes has to get into whether what people are being informed about is actually good or bad for them to do and whether it's dangerous or not.

And then the second thing is that if you see someone with a notice like this, it kind of seems like they want people to fall off the cliff. And that, I think, is a real problem.

So for enforcement, the last thing to add is that we have seen scores of violations of the ALPR privacy law where California law enforcement share with the federal government. That is an example of how once you have the information, even -- even if there's a law saying that it

may not be shared, that sharing still happens.

Second, under many laws, including the CCPA, the lack of a PRA does hamstring enforcement. And, you know, going back to the Attorney General's letter in 2018, when the CCPA was being passed, a private right of action is a necessary complement, in General Becerra's words, to AG and agency enforcement.

Thanks very much. And yeah, happy to take questions.

CHAIR URBAN: Wonderful. Thank you, Mr. Snow. We'll move right along to Ms. Dwyer and Mr. Bowman from the Center for Democracy and Technology. I'll just highlight that Ms. Dwyer is a policy analyst with CDT's Equity in Civic Technology Project, and Mr. Bowman is a policy counsel with CDT Security and Surveillance Project.

And I will ask -- I will turn things over to you and, again, ask you to try to keep it to about 10 minutes. Thank you very much.

MR. BOWMAN: Absolutely. And thank you so much for the opportunity to be here. It's an absolute pleasure. For a little bit of background about CDT, the Center for Democracy and Technology is a nonprofit organization based in Washington, D.C Our team is a mix of technologists, legal experts, and policy experts who are always going to keep our work grounded in equity and

democratic values.

We do have a partner office over in the -- over in Belgium that we work with quite frequently, but Maddy and I are both based in our US office. Personally, my background is all in criminal law. Prior to working at CDT on tech policy issues, I was a public defender. And so at CDT, my work focuses primarily on law enforcement use of surveillance technology and law enforcement use of personal data in criminal investigations and prosecutions.

I'm going to be talking a little bit today about federal access to CAI, Commercially Available Information, through data brokers. And frankly, I'm quite relieved that we've had some wonderful presentations from our -- some of our other presenters, which means that I had to skip over quite a bit of the -- the background and focus a little bit more on two issues that I think might be of interest to the Board. One, particularly how AI can be used to transform all of the problems that we've already discussed. And then two, a couple of the particular policy solutions that I think are worth going into a little bit more detail.

I want to first point out that CDT has been working on data broker issues for quite a while. Down at the bottom of the slide, you'll see a CDT resource, 'Legal Loopholes and Data for Dollars'. This was some

investigative reporting that we basically did, or investigative research that we did, that looked to map out what actually is the landscape of the federal law enforcement agencies acquiring commercially available information.

And in that report, we talked about 30 different publicly available awards or grants that we had found from recent years, which totaled about $86 million in awards. But frankly, that is just the tip of the iceberg, in our opinion. We think that in reality, the annual federal law enforcement agency spend on commercially available information is likely in the hundreds of millions of dollars.

When I talk about the data broker landscape, I think we've gotten a good picture of how that -- there's a mix of global giants and these highly specialized firms. And I think that the differences between these different categories are not necessarily that nuanced. What I mean is that, you know, some can obviously be in both. And we've heard quite a bit about that.

Now, the government does like to pick out a handful of particular data brokers that it likes to use, and that's -- you know, it's hard to say exactly why, but sometimes it's about the sensitivity of the information or it's the availability of commercial off-the-shelf

contracts for which that information can be accessed. So I've listed a couple of them there.

One trend though that I would really like to highlight is that in recent years, we've seen the federal law enforcement agencies pursuing more and more unstructured data. So we've heard a lot about all of the different structured data that data brokers might have on individuals. These are things that fit neatly into Excel spreadsheets, a device ID, a GPS coordinate, you know, a particular address.

What is becoming more and more interesting to federal law enforcement is unstructured data, sentiments, ideas, the things that you are posting on social media summarized into a dossier that can be used basically against you. And I think that this is going to continue to explode in the coming years.

We've heard a lot about how data brokers get your data. I think it's good to just kind of reiterate those three main points: the surreptitious harvesting via SDKs; the automatic leakage that happens from real-time bidding, and I think David's probably going to be able to talk a little bit more about some of the issues there; and then the mass aggregation of public records.

I do want to highlight one more point on scraping that I think the Board might be well familiar with, but

many brokers engage in practices of scraping or mining data that they claim is publicly available, and then they, you know, repackage it and sell it. But this might be in clear violation of terms of service, especially with social media companies.

We've got numerous examples of this happening. Clearview AI, which received cease and desist letters from several social networking companies regarding this practice; or Dataminr is another big one, which frankly publicly claims to mine 10,000 datasets, and this was according to Freedom of Information Act documents that were obtained by Just Futures Law.

And the reason why I highlight this is because in many contexts, the private -- private policies or privacy policies, and the general laws against unfair and deceptive trade practices that we heard about from Commissioner Slaughter, are the only real protections that apply to this data. You know, individuals may maintain a set of expectations regarding their relationship with the first firm in a data supply chain, but frankly have little or no knowledge of how that firm has shared downstream to aggregators or brokers who then might go on and sell that data to the government.

And so in many contexts, those contractual provisions may limit the ability of data brokers to share

the personal information, but the general rule is that once these brokers have obtained the digital information, the only protectors come from the brokers' own opaque privacy policies. And so frankly, that leaves open the door for the ultimate purchaser, the federal government, to come in and -- and take advantage of it.

Now, I -- I talked a little bit about unstructured data, and I want to talk a little bit more about how AI can transform data. Increasingly, we're seeing data brokers use machine learning to combine fragments of your -- your data, your digital life, into a much more comprehensive profile. And AI can identify patterns across different datasets to reveal your real-world identities. And frankly, this has a lot of different applications.

Over the last couple of weeks, one of the most interesting parts of my work has been going to Hill offices, meeting with members of Congress, and demonstrating the ways in which this is really, frankly, quite easy and accessible. So we've partnered with an organization called CivAI, which has put together a demonstration which shows the ways in which agentic AI can be used to browse many data brokers' databases at once and create these highly revealing dossiers of individuals.

So, you know, we're no longer just going to

Equifax and buying your financial history, and we're no longer just going to Dataminr and scraping your social media, but we're combining it all into one. And so here's an example that I would put together. It's very easy, frankly, right now, today, with a little bit of, like, technical expertise to -- to -- to develop a system and basically say, "Create a list of high-profile targets that are, for example, reproductive healthcare providers in a particular town in California.

"Now -- now aggregate all of the commercially available information for these reproductive healthcare providers and create a dossier. And then go to a geolocation provider and then correlate their information so that we can map out their activities. We get a sense of their life." And within seconds, an AI system can generate a dossier that says, "Here's everything you need to know about these reproductive healthcare providers," including where they go, where they sleep at night, their children, where their children go, all these kinds of things.

And all of this can be done in parallel. I mean, AI systems are very good at running multiple operations at once. And so it's very easy to create these much more comprehensive lists that frankly present privacy concerns that we've rejected for hundreds and hundreds of years.

And this is a conversation I often bring in with conservative partners is that, you know, look, there are -- there are -- we -- we have resisted since the founding of the Constitution, the creation of national registries of things like gun ownership, of things like people with disabilities, of things like people who seek certain types of healthcare. We've resisted that for hundreds and hundreds of years, and AI and commercially available information is now making that possible, and the law simply hasn't kept up.

Now, how the government actually gets this data, you know, they're often using commercial off-the-shelf contracts with these data brokers. A lot of our research has unveiled how, frankly, in many, many cases, the government uses very vague budget categories and opaque terms. They'll say something is open source or publicly available information to describe the data, but frankly, this really obscures what's actually going on here.

You know, information that's characterized as open source or publicly available may not actually be readily available to the public, and as we've seen from some of the other presenters, actually requires quite specialized companies to conduct research and collect data specifically to meet the terms of a government contract. And yet, the federal government is going to report it as

commercially available information, publicly available information, or open source, to try to kind of hide what's going on here directly.

I also want to point out that we're seeing an increasing trend where data brokers themselves are not contracting directly with federal agencies but provide databases through different vendors. So in some circumstances, a vendor who contracts with agencies might actually acquire data from other companies and may also provide its broker services through intermediary companies.

An example that comes to mind is Venntel, which we've seen on a couple of other slides here. Venntel sells location data to several federal agencies, but it also acquires data from other countries. And it offers the same underlying data through another broker called Babel Street, which uses a particular product called Locate X.

And it feels like I'm just, like, saying a bunch of jargon here, but I think part of the point that I'm giving is that oftentimes this data just gets repackaged by more or less the same entities to try to avoid scrutiny.

We've heard a little bit about the data broker loophole. How often does the government actually exploit

it? Again, I think that annually the answer is probably in hundreds of millions of dollars spent on purchasing data from data brokers. In 2021, again, we reported on $86 million from just 30 awards that we think is a relatively small proportion.

How we close the data broker loophole? Frankly, I think the best answer is a bill called the Fourth Amendment Is Not for Sale Act. It was first introduced in 2021. It had bipartisan support. In fact, in April of 2024, it passed the House and then later stalled in the Senate after being narrowly defeated in the FISA reauthorization debate.

Speaking of FISA, if you have been checking your notifications throughout the meeting, we had -- just have another 45-day extension of FISA. Several of the main legislative proposals that would authorize it for much longer include the Fourth Amendment's Not for Sale Act as one component of the reauthorizing legislation.

I'll talk a little bit more about the Fourth Amendment's Not for Sale Act in a second, but real quick, I just want to mention that what states can do, you can pick up the mantle. In 2025, Montana became the first state to pass a version of the Fourth Amendment's Not for Sale Act, and I think we're going to see more and more to come, and it would complement, frankly, California's

privacy regimes quite well.

There are four basic provisions within the Fourth Amendment's Not for Sale Act. The first is to expand the definition of covered entities under the Stored Communications Act to include intermarry -- intermediary service providers, specifically with a mind of including data brokers, but keeping the term a little more broad to include the wide variety -- a wide category of providers.

The next is to add a general prohibition on law enforcement agencies and elements of the -- of the intelligence community from actually purchasing covered records. And this would include any illegitimately obtained information from third parties -- and any information from third parties.

This is important because we've actually seen reports of the federal government purchasing data that was exposed through data breaches, for example. And frankly, that's a -- a no-brainer that we should close that opportunity off.

The third is to introduce an exclusionary rule that prohibits the use of court -- in court, of any evidence derived from or obtained in violation of the statute. And the fourth is to prohibit dissemination of information obtained in violation of the statute to other federal agencies.

Oftentimes, you know, we see this, frankly, in regular routine investigations, the idea of parallel construction, which is that law enforcement will say, "Well, we actually got this information somewhere else because we corroborated it after we received it in the first place." And so this is to shut that down a little bit.

I'll pass it off to Maddie here. I do want to say one last thing that I forgot to mention is that when I was talking -- when I'm thinking about the evolution of how the federal government actually contracts with data brokers, what I'm seeing is more and more of integration of what we think of as data broker service into other intelligence platforms.

So law enforcement across the country are being marketed to these platforms that use AI in a wide variety of ways, some of which isn't necessarily relevant to data brokers. You know, we talk about using AI for transcription of body-worn cameras or for the generation of police reports. But many of these platforms that are meant to be like evidence and case management platforms are actually coming preloaded with advertising intelligence, business intelligence, and other data that is essentially being provided by data brokers.

So again, to try to skirt any sort of

transparency or accountability, data brokers are actually selling their data to these platforms who are then the entities that contract with the federal government. And again, this just obscures the relationship between the data exploitation and then the federal law enforcement agencies using it.

I've been over time. I'll end there and I'll pass it off to Abby.

CHAIR URBAN: Yeah. I need to do it -- I do need to do a time check. So we are slated to end at 4:00, and I'm wondering if Board members can stay a little bit longer because I do want to be sure that we have time to talk with our panelists, and I want to be sure the public has a chance to comment. Okay, thank you.

And thank you, Mr. Bowman, for recognizing that. And I will ask our remaining two speakers to also be thoughtful about that. I'm sure you want lots of questions from us. And with that, Ms. Dwyer, please go ahead.

MS. DWYER: Awesome. Can you see my slides?

CHAIR URBAN: Not quite, but it often takes them a second to appear, so let's see.

MS. DWYER: Let me try one more time. If not, I might need Tom to take up the mantle for the slides. Tom, do you mind sharing the slides?

CHAIR URBAN: There we go.

MS. DWYER: Perfect. Thank you so much. So I'm going to shift a little bit away from commercially available information and talk about the issue of federal access and consolidation of state-level administrative data.

And I'm -- I'm talking about this issue today because on top of what everyone shared that is quite concerning, I think pairing this part of federal access to Americans' personal data makes the issue even more concerning when you think about the fact that you can layer both commercially available information and information that's held directly by the federal and state governments to build these profiles on individuals, use it for things like immigration enforcement purposes.

So I'll start really high level with what is administrative data. So it's information collected by federal, state, local, tribal, territorial governments that is used to -- that is collected and used for services and benefits for constituents within states, and then for programs administered by the federal government.

Oftentimes, administrative data includes really sensitive personal information that basically creates a story of someone's identity in life. So this includes things like Social Security number, someone's employment

history, where they live, how many people are in their household, whether they've had a death in the family; the list goes on and on.

And oftentimes information that's actually held by public agencies is more sensitive because they have access to things like a direct Social Security number, and it is collected directly from the person and not necessarily inferred by all the different data elements that are -- were mentioned earlier. Next slide, please.

So this slide is just to say this is not a new issue by any means. Federal efforts to access sensitive state data, which has historically been held and safeguarded at the state level, have really accelerated over the past few decades. So we've seen this happen both in the Bush and Obama administration for things like immigration enforcement.

But what's different about what we're seeing today, which if you go to the next slide I can show, is that since January 2025, these efforts have really ramped up, have scaled up, and have been really more concerning because of what Tom had mentioned about the use of AI to build these sort of dossiers or profiles of individuals.

So it really started in January of 2025 with the US Department of Government Efficiency basically ransacking federal agencies' databases, trying to get

information on individuals. And, you know, since the DOGE era disbanded, the efforts have continued and the Administration has expanded its efforts to actually go after states and try to get access to state administrative data.

So this effort actually really began in full force on March of 2025 when the Trump Administration issued an executive order directing federal agencies to get access to state administrative data run by different benefits programs that receive federal funding. And this has actually included trying to get access to this data via third-party EBT vendors for programs like SNAP, Medicaid, etc.

So we've seen over the course of months and up until now, the Administration has requested SNAP data, Medicaid data, and unemployment insurance data databases to try and get some of the most sensitive information that they can get about Americans across the country.

And in the SNAP case in particular, one of the things that happened was USDA sent a letter to every single state demanding, you know, "Give us access to this information about beneficiaries, including their names, Social Security numbers, and addresses," and also said that they were going after the third-party vendors of EBT to get this information, which is something that has not

been seen before. Next slide, please.

So there are a number of ways that, you know, states can address this issue directly. I will say that there's a lot of legal requirements for the federal requests for this data, including the Privacy Act of 1974, which was referenced earlier, the Paperwork Reduction Act, and the E-Government Act.

And then states also have their own legal requirements when it comes to actually responding to these requests, like their privacy laws, sector-specific federal privacy laws like HIPAA if it comes to health data, and in addition, state contracts with these EBT payment processors vendors.

One of the ways that we've seen states sort of respond to this renewed request for information at the state level is introducing legislation. So in the last session, we looked at every single bill that was introduced on this topic to try and either strengthen or weaken privacy protections. So we saw that 79 bills were introduced across 29 states and 17 were enacted. And next slide, please.

So I'll just go briefly through some of the ways that states in legislation have tried to address the Trump Administration's renewed push to gain access to state administrative data. The first is just increasing general

privacy and cybersecurity protections.

So this includes updating or even just putting into place Privacy Act-style laws that California has. California has a very strong -- one of the strongest ones out of all 50 states -- called the California Information Practices Act of 1977. Another really important piece of the puzzle is safeguarding immigration-related information by actually prohibiting voluntary sharing with federal immigration authorities.

The third, we saw legislation introduced responding directly to DOGE's threats, saying, you know, "We need to be stewards of privacy and ensure that our constituents' data is being safeguarded."

The fourth is protecting education-related data. As we saw earlier through a presentation, there's been attempts to detain folks at schools, so doing a better job of saying, "Hey, schools, you know, do things like data minimization and actually prohibiting collection of student citizenship status unless required by other laws." Next slide.

Some other areas is safeguarding disability status information, increasing privacy protections for tax-related information, and then I'll call out some additional areas is protecting data related to sexual orientation and gender identity, which California passed

last session, SB59. And this makes court records related to an individual's name or gender marker changes confidential. And next slide, please.

So with all of that, you know, we looked at all these bills and we tried to say, you know, "What are the top the top five things that state policymakers, you know, other state officials issuing guidance or rulemaking can do to protect their constituents' data from these federal requests?"

So a lot of these concepts are -- have been introduced by the other speakers. First is data governance; so having things like maintaining our records of what all -- what are the systems of information that you have; what are the categories of information sensitivity levels that are in those systems; and who has access to those systems?

The second is, of course, data minimization and disclosure; so really limiting the personal information that's collected and disclosed on an individual to only that which is necessary for the intended purpose. And then notice, access, correction; so providing people with notice when their information is being used and shared with third-party entities like other agencies or other vendors.

The fourth policy priority is data retention and

deletion. So this is limiting the time period for which information is retained and using best practices to delete personal information. That reduces the -- it reduces the overall amount of sensitive information held by the government.

And lastly is enforcement mechanisms. So, one of these that we are strong advocates for on the government data privacy side is, of course, a private right of action; so, giving individuals the right to sue to protect their rights when an agency or individual violates their government data privacy protections.

And I will leave it there. And looking forward to questions.

CHAIR URBAN: Thank you very much, Ms. Dwyer. Last but by far not least, we have Mr. David LeDuc, who's Vice President of Public Policy with the Network Advertising Initiative. And I will turn it over to you, Mr. LeDuc, with, again, my thanks for your patience, and we look forward to what you have to say.

MR. LEDUC: Well, thank you, Chair Urban, Board members. Really appreciate the opportunity to be here today, being included in this important discussion. I want to start out by talking a bit about the NAI to provide an overview of who we are and what we do. If you'd go to the next slide, and thanks for driving for me.

So the NAI was founded in the year 2000, 25 years ago. We've been the leading self-regulatory organization working at the intersection of privacy, technology, and public policy to promote heightened standards across the advertising technology ecosystem.

And our mission is essentially three different pillars: We focus on providing practical guidance for our member companies to help them navigate the complex and rapidly evolving legal landscape; we build a culture of privacy that promotes the trust and privacy as foundations, as competitive advantages across the industry; and we engage with federal and state policymakers like yourselves and others to promote policies that meaningfully protect consumers, while at the same time not inadvertently destroying data-driven advertising, the -- the system that keeps digital content free and available to so many Americans.

There's one thing I want to be clear at -- at the outset: the NAI is not a typical trade association. We are a self-regulatory organization committed to providing our members with independent privacy reviews and promoting their compliance with enforceable laws and regulations. We are a tool to help you and other enforcement agencies that are the cops on the beat, and that's a new model that we've adopted beginning last year.

If you go to the next slide, I'll do -- I'll provide an overview of the NAI's position, and I think you'll be pleased to hear that it's consistent with a lot of what you've heard today, that we oppose non-consensual sharing of consumer data for law enforcement. We've long opposed this. We've taken concrete steps to address it.

In 2020, we first published a set of best practices providing transparency guidelines around personal information collected for advertising that's also shared for other purposes. At that time, you know, we had a code of conduct that was created only for advertising uses, so we developed this set of best practices to go beyond that as we realized that there -- there -- there were additional uses arising in the marketplace.

And then in 2022, prior to the Dobbs decision, we published 'Voluntary Enhanced Standards' specifically designed to increase privacy protections for consumers' precise location information, including explicit restrictions on participating companies from using, selling, or sharing any US consumer's precise location information with law enforcement or national security purposes.

Our concern regarding this -- this sharing is that it's rooted in a straightforward principle: consumer data is collected under commercial expectation. When a

consumer decides not to opt in or not to opt out of interest-based advertising, or affirmatively opts in to share their sensitive data, such as in location-based services, they are making a choice based on commercial terms; the understanding that their data will be used to power digital media and services and to show relevant advertising. They're not agreeing to have their data repurposed as a tool of government surveillance.

The harms from allowing this repurposing are real. It violates purpose limitation principles that form the bedrock of modern privacy law, and it creates a chilling effect on lawful online activity. There's also significant risk this activity will disproportionately impact vulnerable communities, as you know -- immigrants, people seeking reproductive healthcare, religious minorities who face the greatest risks. That's a big concern of the NAI's as well.

We recognize that most businesses do not choose to engage in this practice, but it only takes a few companies willing to gather consumer data and sell to the government agencies to undermine trust in the entire digital advertising ecosystem, which in -- is the situation we face today, unfortunately. This is a collective action problem, and it calls for public policy solutions.

We encourage the Agency to address this problem, but to do so in a targeted way, proportionate way, that does not have the unintended consequences of restricting valuable privacy-protective uses of consumer data. The NAI believes that public policies can prevent advertising data from feeding a government surveillance infrastructure without effectively banning data-driven advertising.

So moving on to existing laws, I'd like to spend a bit of time here because I think these are -- these are important aspects that are -- that are directly focused to -- to the Agency. Obviously, existing law provides an incomplete, you know, set of tools, but -- but it does provide a strong foundation. So I want to talk specifically about some of the specific tools that you all have that are unique.

You are the nation's leading consumer data protection organization across the states, and you have tools that are already available and are very powerful. We see two complementary approaches, and they've been talked about a bit today, and to some extent I think, you know, there's been a fair amount of discussion about how transparency and control don't do enough.

And we don't disagree with that, but I do want to spend some time highlighting what they -- what they can and do accomplish. So the first thing I want focus on is

increasing transparency and consumer control so that consumers can take additional steps to identify bad actors and exercise their rights.

And the second is talking a bit about how you can establish clear restrictions on sharing and prohibit law enforcement agencies from obtaining this information. On the transparency and control front, the CCPA's Core Consumer Rights framework is directly relevant. If consumers are informed their business shares their data with government agencies, they can make choices based on that information, recognizing these choices are limited, but again, you have a special set of tools.

In conjunction with the CCPA's purpose limitation principle provides -- in conjunction with the transparency, the purpose limitation principle provides a very strong tool to restrict nonconsensual sharing with law enforcement. For example, Section 7002 of the CCPA regulations requires that collection, use, retention, sharing of personal information be reasonably necessary and proportionate to achieve the purpose for which personal information was collected or processed. This includes considering whether the processing or sharing is consistent with the reasonable expectation of the consumer. This is something that I expect, you know, quite well.

Collecting and processing personal information to power commercial services and the data-driven advertising that supports these services is well-established practice whereby disclosed purposes and expectations align. However, collecting personal information for commercial purposes, then choosing to share it with law enforcement, is plainly neither reasonably necessary nor consistent with the consumer's reasonable expectations.

This inconsistency becomes exacerbated when the sharing involves sensitive data such as sensitive health data or precise location data. Law enforcement use is categorically different, and a business that shares data for that purpose without a completely separate and distinct disclosure is, we would argue, acting inconsistently with the CCPA.

This agency has the authority to explicitly declare this as unlawful under the CCPA. The Agency could issue clear guidance that the practice of sharing data with law enforcement would need to be accompanied by a separate, distinct notice, which would provide consumers with the opportunity to accept or reject this practice at the outset.

Additionally, and very importantly, the DELETE Act's new transparency requirements are a very powerful step in this direction, now requiring registered data

brokers to disclose in greater detail the types of data that they collect and with whom they share this data.

However, there are open questions, we believe, about the DELETE Act and how it applies to companies that sell California's personal information to -- to the government. Under current law, there appears to be ambiguity about whether a business that sells personal information only to the government is selling to a, quote, third party, under the law and is therefore required to be classified as a data broker and registered.

As a result, it's not clear that companies in that category are required to register in California. Providing clarity on that -- on that issue by amending the definition of third party to clearly apply to government entities, could immediately bring these companies in the category and make sure they're registered and are held under transparency and accountability requirements of the DELETE Act.

This is a really straightforward and important point that if you have not considered, we hope that you will take a close look at and consider. And then if you go to the next slide, definitely agree that there are limitations with transparency and control, but they are important, and your law and other laws do focus on them, and we all, I think, agree to -- to make them as strong

and effective as possible.

But what should new legislation look like? We -- we believe very much -- there's significant agreement between the NAI and what you heard from our -- our colleagues at the CDT. Ideally, the federal government will enact clear rules for law enforcement access and on use of commercially available information to alleviate these privacy risks.

However, until such time as -- as that takes place, the NAI fully supports the efforts at the federal and state level to restrict those agencies from accessing this data. At the federal level, we also strongly support the Fourth Amendment Is Not for Sale Act that you just heard about. Thank you to my colleagues for providing the overview, and I don't have to do that.

We also believe that state legislatures can take a parallel approach as well by both promoting similar policies or promoting policies that -- that -- that prohibit the -- the sharing from the commercial side to the government. Those are two different -- you know, two different approaches, and to some respects it's stronger to put the prohibitions on -- on the companies because the -- the sharing can also be with non-US entities and bad actors. So that's another important complement.

So if you go to the next slide. I'd like to

offer a caution, however, and -- and -- and offer a plea for targeted solutions. I can't overstate the important risk that the Agency and legislature face as you consider next steps, alternative policies. Several states have recently enacted sweeping restrictions on the collection, processing, and sale of consumer data, particularly but not exclusively around precise location information, precluding many legitimate and privacy-protective commercial uses.

Maryland, Oregon, and Virginia, as you may know, have all taken steps in this direction, and other states are considering it, as is California actively.

I'd like to highlight a bill that I know that you have supported, AB322, and I'd like to talk a bit about what it does, where we feel like it does right and where we feel like it goes too far. We -- we oppose the Bill as currently drafted because we feel that it would create an outright ban -- we know that it would create an outright ban on sales of precise location information -- and this would curtail legitimate advertising and app functionality.

However, we strongly support the Bill's provisions that would prohibit commercial sharing of -- off precise location data with law enforcement agencies, and that is exactly the kind of narrowly tailored

restrictions that we're advocating for today and in the future.

And similarly, I'd like to talk about AB1542 that I know you will be considering tomorrow, whether or not take a position in support of that. This creates an even broader ban prohibiting the sale of all sensitive personal information. Again, the NAI is highly concerned that these types of blanket prohibitions have unintended consequences.

Strict limits on the selling and sharing of all sensitive personal information, such as precise location data or sensitive health data, would disrupt many legitimate and responsible uses of this data that benefit consumers and provide for a competitive marketplace.

For instance, location solution providers enable free and low-cost app functionality for millions of consumers. I appreciate the presentations earlier talking about the data flows. I think that was very helpful to provide a frame of how different entities work together across the marketplace, and it's very important.

And a lot of these blanket bans would shut down a lot of those data flows entirely, prohibiting a lot of the beneficial uses that were discussed in addition to the harmful ones that we're -- we're all trying to avoid.

One of the points I'd like to make also in this

area before I move with it -- before I move on is about the largest technology providers getting a competitive advantage. They provide their own location-based services through vertically integrated systems. They don't rely on third parties. They've got a bunch of their own technology and their own customers.

The result ends up being from these types of policies to -- to -- to just exacerbate the market imbalance and concentrate more power in the hands of the few largest companies, curtailing services from small and medium-sized publishers. And we know that's not what you want. We don't think that's what anybody wants.

The -- the policy objective here is to prevent advertising data from being weaponized for law enforcement and surveillance, and we believe that can be achieved through more narrow policies that are reasonably scoped. Broad prohibitions on -- on data sharing could also conflict with First Amendment speech protections, which safeguard the legal ability of -- to share lawfully acquired data.

Instead, a more targeted ban, such as one focused on sharing with law enforcement, would better align this fundamental US constitutional principle, with generally -- which general calls -- which generally calls for least restrictive means possible of meeting legitimate policy

aims.

And this is an important point that I think a lot of policymakers are overlooking with respect to these broader policies. There's a very significant possibility that these will be challenged in court and overturned anyway on these grounds. And another good reason, we believe, for focusing policies more narrowly to achieve -- to address the specific harms and misuses.

So if you would go to the next slide, I'll just say in conclusion, our message today is simple. We really appreciate the opportunity to be here. Consumer data collected to power digital services and related advertising should not become raw material for government surveillance. This is inconsistent with the purpose for which it was collected, and it threatens trust and the foundation of the entire data-driven economy.

We're encouraged by the Agency's track record of vigorous enforcement, and we believe that a combination of agency guidance, targeted amendments to the DELETE Act and CCPA, and carefully scoped legislation can address this problem effectively.

The NAI, our members, the rest of the industry -- we stand ready to work with the agency, the legislature, and our counterparts in the privacy community to develop

these solutions. We're happy to share model language,

additional technical expertise, explain how advertising data flows work, and our experience developing enforceable self-regulatory standards.

Again, I really appreciate the opportunity to be here, that you're including our self-regulatory industry perspective, and I'm happy to take any questions along with my -- my colleagues.

CHAIR URBAN: Thank you very much, Mr. LeDuc. All of those presentations were illuminating, concrete, and helpful. Thank you so much. Are there questions from Board members? Ms. Ozer? I have a few, but I won't start.

MR. LIEBERT: And they're for all of the various panelists?

CHAIR URBAN: I think you can ask of them, of whoever seems appropriate. Yeah.

MR. LIEBERT: Okay. Let me start with you, Mr. Snow. Thank you for being here. That was a great, great presentation. I -- I -- I just heard from Mr. LeDuc, a cynicism about the location-tracking legislation that the State is currently considering, I believe, and I don't think you had a chance in your presentation to discuss that.

But I wanted to get -- get your take on that because it seemed to me, based upon your presentation,

that you thought that that actually could make quite a dent in addressing some of the issues that you raised.

MR. SNOW: Thanks so much for the question. And yeah, the -- so AB 322 does put in place a fairly strong ban against the sale of location information, precise location information. And -- and -- and yeah, Mr. LeDuc did talk about the -- the -- the positive uses for that and lifted up some of the concerns around a ban like the one in AB 322.

You know, from my perspective, it's worth thinking about how some of those services, app-based services, can be -- can still be protected and still be funded by advertising without having the privacy impacts that we've all been talking about today and -- and that are so concerning.

You know, having precise location information or other kinds of deeply personal data being extracted from an app and then used to target ads may provide some funding to apps. In fact, it does. It provides funding to other content providers as well.

But also, that similar amount of funding could be provided through contextual ads or ads that do not extract any private data, location information, precise location information. And you can have a -- a -- a debate about whether the amount of funding that would be possible to

generate through contextual or private ads would be, you know, up to the task of fully funding all of the app ecosystems that we've seen.

But I do think that there -- it's an important part of the conversation to remember that advertising as a business model has existed for a very long time. Hyper-targeted advertising based on people's behavioral characteristics and their precise geolocation is a comparatively new phenomenon, and ad-based business models that provide free services or free content to consumers are not something that will go away if you have strong privacy laws.

CHAIR URBAN: Thank you, Mr. Snow. Could I ask a quick follow-up, Mr. Liebert? Would that be all right? I actually have it for Mr. LeDuc. I was curious about the phrase privacy protective on your slides, and it connects directly to this question, I think, about, you know, what kind of data needs to be collected, how would it need to be treated. And I'd like to invite you to unpack that a little bit for us.

MR. LEDUC: Well, I think, you know, in terms of our -- our self-regulatory approach, privacy protective, I mean, now we have a new approach in our program across the NAI, and it aligns with -- with your law and other laws. So to us, privacy protective means in compliance with the

CCPA, in compliance with the DELETE Act, in compliance with all the other state laws, implementing all the transparency and control requirements that you have, implementing all of the other consumer controls that are in these laws, implementing data protection assessments, implementing data minimization requirements, being good stewards of data, not selling it to the government.

So it's really, when we say privacy protective, we mean doing these things that -- that policymakers, not just the industry, has made up. You know, our whole program is based on helping companies comply with your laws. So that -- that's what privacy protective means to us. It means complying with your laws, doing what -- doing what's required, being responsible.

And in this case, quite frankly, in our opinion, it means, you know, in some cases, we're encouraging companies to do more in this area, particularly where not sharing with the government, we think, is for law enforcement purposes, we think is an important step. And we want the laws to catch up.

CHAIR URBAN: Thank you. Sorry, Mr. Liebert, please go ahead.

MR. LIEBERT: No. It's okay, because my question was going to be for Mr. LeDuc, and that is, do you really think that consumers typically are comfortable with the

thought that all of their location data is being shared and -- and whether or not this idea of the opt-in requirement really works in that situation?

MR. LEDUC: Well, I think it varies. I mean, I think it's fair to -- to say that consumer expectations vary. I do really believe that consumers appreciate and enjoy location-based services, the breadth of them, location-based advertising. I think we've all become more and more reliant on that.

I don't think most consumers recognize how much sharing of that data takes place. Again, the diagram that we saw earlier, I don't think most people realize that. I don't think most, you know, well-informed people realize, you know, the -- the degree of sharing, but that's a fundamental reality.

And I would also note that I think it's a bit of a false bargain, the notion that the genie can be put back in the bottle. A lot of data sharing is just a key element of -- of the way various applications work and work together. And -- and it's really very hard, if not impossible, to provide a lot of these services without a substantial amount of data sharing.

Hence, again, citing back to -- to one of those graphs that we saw where there's just a need to share a certain amount of information to different SDKs that are

-- that are functioning for very useful purposes throughout apps.

So I just -- I think, you know -- I think awareness isn't -- isn't where it needs to be. I think that's why some of these new requirements, transparency requirements, are strong. I know that you all are considering, and we're commenting on, making some new -- new regulations around notice and -- and to -- to help aid notice and choice, and that's something that we're supportive of. We think that could be improved, and we're happy to work with you in doing that.

And I think, you know, we're all in it together in terms in terms of helping consumers know how their data is being collected, used, and -- and making choices about it.

CHAIR URBAN: Thank you. Ms. Ozer, was that a hand? Yes. Please go ahead.

MS. OZER: I just had a quick follow-up question for Mr. LeDuc as well. When you talk about sort of ensuring that there's actual consensual sharing of consumer data for law enforcement purposes, do you all see that given sort of the lack of understanding and transparency, that that would be an opt-in or an opt-out mechanism? What makes it consensual in your mind?

MR. LEDUC: Well, a lot of people have debated

your regulations, and I know that you all have, and I've been -- I've been following them since day one and everything that you've all done since day one.

I think there's a really fair argument that your current law and regulations dictate that that would be opt-in, because that would be an opt-in requirement because it's outside of the expectations, and that a simple notice wouldn't suffice, so.

But I leave that to you, and we're happy to engage with you on that. But I think for this purpose, you know, sharing for law enforcement purposes, I think -- I think you all crafted a very strong law, and I -- and I hear you tout it a lot, and I hear others tout it, and I -- and I -- and I don't disagree in -- in this area that the law could be used in -- in a stronger way than it currently is.

And again, I want to also mention the DELETE Act, I think, you know, the -- the amendments that you made there, or the legislature made, and these enhanced disclosures are incredibly valuable. We all saw the disclosures that came out of that, and we know how powerful and effective the -- the drop can and will be, I think most of us think.

Making sure that that transparency is used to the greatest extent possible, that -- that companies that are

engaging in -- in these types of activities are included and -- and are able to have consumers -- you know, of all the data brokers that consumers might want to opt out of, I imagine that it's those -- those companies the most.

So making sure that those companies are looped in, and I'm confident that you all -- you all can do that. I think those tools are -- they're not going to solve all the problems, you know, but -- but I think they're quite powerful and perhaps more so than -- than -- than they're being utilized today.

MS. OZER: Yeah, I just wanted to clarify because obviously there's -- there's a substantive provision that, you know, prohibits the voluntary sharing, and then there can be a notice-and-consent framework, and what that notice-and-consent framework is can also be opt-in or opt-out.

So I wanted to understand where your positions were on the issue of information collected for consumer purposes then being voluntarily shared with the government and where you think sort of the right protections are for individuals.

MR. LEDUC: I -- I -- I personally think that, you know, that that warrant an opt-in under the CCPA as it exists today.

MS. OZER: And then one landscape question also

just for Ms. Dwyer. In terms of the administrative data, have you all done any research or looking into the type of administrative data that's being held at the local level, at cities and counties, versus at the state level and sort of that level of information and sort of vulnerabilities?

MS. DWYER: Absolutely. So we haven't looked specifically from our knowledge of, you know, how a lot of benefits programs are administered. I'd assume at the local level, in some cases, that data could be even more sensitive. So, you know, still collecting things like Social Security number, address, but, you know, I think local agencies, like say in the case of like a child welfare system, you know, has like case information, very specific things on -- on folks.

And one thing I'll note, for example, a lot of the laws that states have that govern administrative data, they do not apply to local governments, and that includes California's Information Practices Act of 1977. So there is vulnerability that local governments could be approached for these sort of requests, especially in states that have strong state-level laws, but again, do not apply to local governments.

There's currently in California a bill that is circulating, it's AB 1337, that would fix that sort of loophole in the current California law that would apply

the current Privacy Act-style bill in California to local governments to fill that gap. And it's one that I hope moves forward and other states recognize the need that local governments also need these privacy protective measures.

CHAIR URBAN: Thank you. This is a question that I think could be for any of you, but I'll start with you, Ms. Dwyer, since you presented a slide that was -- is helpful for framing it, which is the policy priorities for state lawmakers.

And thinking, for example, about data retention and deletion, how do we think about applying those in the context of a large language model, machine learning, sort of generally, the AI world? I'm -- I've been struggling to fit together some of these concepts with the way that some of these technologies work.

I think there's also a related question back -- that relates back to Dr. Good's slide with the complex ecosystem. I take Mr. LeDuc's point absolutely. But it seems that the data, once they're out, they really are in this ecosystem. And then when you get to an AI system, maybe it's just trained the model, and then although you could return it, if you look, it's hard to know how some of these tools might -- might apply.

And if any of you have comments on that, I would

be -- I would be glad to hear them.

MS. DWYER: Yeah, I'll let my colleagues talk about the commercial sort of data retention deletion, but at least from the public sector side, when we're talking about government-held data, one really important mechanism is, you know, it's not really pretty, but the procurement process of actually putting in place contracts between state governments and AI vendors, specifically saying that the government has ownership of the data that might be used in large language models, and that cannot be used for any other purposes, to sell individuals' data, et cetera.

And yeah, so that's a really important lever that we talk about a lot -- is ensuring that the contracts that are in place with AI vendors at the state level is really solid in terms of data ownership.

CHAIR URBAN: Thank you. Other responses, maybe on the commercial side, from maybe Mr. Bowman, or Mr. Snow, or Mr. LeDuc? Mr. Snow, please go ahead.

MR. SNOW: So, I mean, one of the kind of foundational things that privacy law should take into account when it comes to AI models is just the -- the basic notion that training an AI model is a secondary use that is often going to be outside of the purpose for which it was collected.

And, you know, one example of that is a company

that collected a whole bunch of people's family photos as part of a photo app. It's called EverAlbum. And they used all of those photos, billions of photos ultimately, to analyze using facial recognition so that people could see, you know, all the pictures of their cousin, or something, in a family photo album.

And then they used all of those images to train a facial recognition system, build a facial recognition product, and then try to sell that facial recognition product to the military. They were covered in the press. There was an FTC enforcement action about them. They eventually shut down the consumer product and just had the surveillance product.

And to me, that that is the sort of, like -- that is the dark turn of a consumer-facing company collecting information about people, collecting a whole bunch of private information, and then turning away from that to become what is effectively a -- a military or government contractor.

We've seen that in lots of different ways. I mean, a lot of presentations today have touched on various variations of that story. But I do think that from the perspective of collecting the information, using that information to train an AI model of any sort would be another secondary use that's outside of the purpose for

which it's collected.

In many instances, it is going to be prohibited by a -- a strong data minimization privacy law.

CHAIR URBAN: Thank you. And do you think that our -- our Section 101 of the Statute, Section 1 -- Section 1100 of the Statute, and our corresponding Section 7002 of the regulations would prohibit that?

MR. SNOW: Yeah. I mean, you know, the -- there is the language in 7002 about, like, reasonably related. And so that would be the sort of practical factual question in any -- any individual case. But I think in many cases, those kinds of training models would be prohibited by the regulations.

CHAIR URBAN: Thank you, Mr. Snow. Other comments? Yes, Mr. Liebert.

MR. LIEBERT: Yes. This one's for Dr. Good. Your presentation was so stimulating and frightening. It seems to me that we haven't had many conversations yet, but it's probably about to hit this agency and -- and many others, and that is the impact of these enormous AI platforms about to engage in advertising themselves.

And given that incredible landscape that you showed us, I was wondering what thinking you have about that, because it seems to me that when you combine the most sensitive and amazing information that so many people

are sharing with these AI systems directly, and then they potentially have the ability to -- to -- to sell or share that information, it's a whole new amplified set of challenges.

MR. GOOD: Yeah. I think Mr. LeDuc, was it, talked about -- talked about this when -- when he was mentioning sort of the power of the verticals that have access to all of this. I think with AI and advertising, the big players have a massive advantage in the sense that they have such an intimate amount of information about their individual users that they -- they -- they don't need to buy and sell that data. They're going to have that.

And I also think that they probably won't sell that data directly, but they'll sell access to that data and -- and -- and use that to monetize it.

So -- so I think, and this is all being very hypothetical, but in those cases, the -- the -- the verticals that have the -- the most amount of information are going to be able to have very sort of intimate knowledge, but I don't think there's a large incentive for them to share it directly as opposed to sort of charge for access to it.

MR. LIEBERT: So -- so just so I understand, the implication I think of what you're saying is -- is that

these AI systems will themselves become the major advertisers directly. They won't need to be selling or sharing, they will be it. So they --

MR. GOOD: Yes.

MR. LIEBERT: -- in essence, will be a huge threat to the current advertising marketplace.

CHAIR URBAN: It's okay, you don't have to -- have to draw a conclusion.

MR. LIEBERT: You don't have to use my language. I'm just -- I'm actually just wondering if --

CHAIR URBAN: It could change the advertising marketplace pretty fundamentally.

MR. GOOD: It -- it -- it definitely could.

MR. LIEBERT: Yeah. Okay. Interesting. Thank you.

MR. GOOD: Of course.

CHAIR URBAN: Thank you. Are we -- did anybody else want to comment on that? Okay. Yes, Ms. Ozer.

MS. OZER: Some of these players are the same players as have been doing this now. So, you know, some of the big companies have so much data that they don't share with data brokers, but they monetize that themselves for lucrative advertising. And some of those people are the same people that now have the AI systems as well, correct?

MR. GOOD: Yep.

CHAIR URBAN: Okay.

MR. LIEBERT: I do not want to leave Mr. Bowman out at all. Your presentation was also great. And one of the things that -- it struck me as you described the landscape that you're dealing with in Washington is that there -- one would think, would be an alliance between the federal government in terms of the data that it is seeking for all sorts of purposes, and the data broker industry, because they're relying very much on the data broker industry to get so much of the information they're seeking to use.

And then the federal government, obviously post-DOGE, has tremendous troves, what is now apparently combined data. I was wondering if you could comment about that.

MR. BOWMAN: Yeah. And you don't have to look too far to see it, right? You know, we -- we've heard reports about Palantir and a particular data management program that they have, Elite, which is suggesting, you know, immigration enforcement targets, apparently, among other things.

But this is kind of this natural coalescence of interests, right? The federal government has an interest in -- in all of this data, data brokers have an interest

in a very stable source of revenue from the US government, and that leads to very lasting relationships.

And it also can lead to entrenchment, which I think is really, really difficult then to uproot, especially if -- I work a lot with law enforcement and one of the hardest things is that once law enforcement has access to a particular tool or to data, it's very hard for them -- to get them to relinquish that access or that grip on it.

So I think it's really, really concerning, and I think that that consolidation is happening quite rapidly and frankly quite publicly. But it's still yet difficult to get both sides of the aisle to agree to act on it. And that's where I think a lot of this is going to come on states, and this is where states can make a lot of ground.

CHAIR URBAN: Thank you, Mr. Bowman. Yes, Mr. LeDuc, please feel free to weigh in.

MR. LEDUC: Thanks. And I'm sorry if this is coming a bit late, but I -- I was going to jump in earlier on the conversation about, you know, the -- the larger technology companies and -- and data sharing, and then -- and the AI, and -- and that conversation kind of evolved a bit.

And I didn't, you know, mean to be saying or speaking much about, you know, the new role of AI and --

and -- and where advertising is going. I mean, that's hard to know. But, you know, to make the point again, you know, that I made earlier and to clarify my point being that, you know, these broad bans that are well-intended, I mean, it makes tons of sense on -- on one level to say, like, "Well, then just, you know, don't -- don't sell the data."

But -- but unfortunately, your law and most of these other laws are literally created in -- in a way that impacts all these other businesses and -- and not -- not those larger platforms, you know, who don't need to sell and share data, you know.

And so -- so these laws, you know, maybe they're having some positive effect, you know, in preventing the selling and sharing. I know what you're trying to accomplish. I know what you're -- you know, the legislators are trying to accomplish, and -- and it's not crazy, but it just has this, you know, I just can't understand --

CHAIR URBAN: Thanks.

MR. LEDUC: -- the effect that it has. So I appreciate that. Thanks.

CHAIR URBAN: Thank you. Thank you, Mr. LeDuc. Sorry. I'm glad we're not crazy, but -- but I do take your point. I do take your point about the limits of the

protections and the practicalities of the marketplace and the different sizes of the players.

I think it's time to turn to public comments. Thank you all, again, for your patience and your energy. I will certainly invite all of the speakers to stick around and listen to what Californians have to say. But I know that some of you, I think some of you are on the East Coast, so I certainly don't want to keep you longer into your evening than we already have if -- if that's not convenient for you.

So I will send you off, if you'd like to go, with my very sincere and the Board's very sincere thanks for the care that you put into your presentations, and the depth and breadth that you brought to us today to aid in our understanding of these crucial issues for Californians and, indeed, for Americans. So thank you very much.

And with that, I will call for public comment. If you would like to participate in person, please stand by the podium to my right, to your left. And when you are called forward, please speak clearly and directly into the microphone because the mics unfortunately can be quite temperamental, and that is the only way for everyone to hear you and for the record to -- the meeting record to capture what you say.

If you would like to participate by Zoom, please

use the raise your hand feature at the bottom of your screen if you have logged on via Zoom. If you have logged on using your phone, please press "star-9", and that will raise your hand on the moderator's view. Our moderator will call you when it is your turn and request that you unmute yourself at that time. Zoom users can use the unmute function on their screen, and phone users should unmute by pressing "star-6". When your comment is completed, the moderator will mute you.

As a reminder, the topic for public comment is the same as the topics for today, so please contain your comments to the topics that we discussed today, the issues that we discussed today. And you have three minutes for your comment.

Ms. Carwile, I'd like to ask that you let us know if we have any public comment.

MS. CARWILE: Again, if you would like to make a comment, please raise your hand by using the raised hand feature or by pressing "star-9" if you're joining us by phone.

MS. CARWILE: I'm not seeing any hands raised at this time.

CHAIR URBAN: Thank you very much, Ms. Carwile.

Again, my deep gratitude to our speakers for today, and I will especially acknowledge the folks here

with us in person, Mr. Snow, Dr. Good, and Ms. Chen, still here with us in person, and to everyone who took the time to listen and to learn with us today. We will now recess until 9:00 a.m. tomorrow, May 1st, when we will continue with the board meeting agenda items.

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

(Whereupon, a recess was taken from the informational session.)