THE BROOKINGS INSTITUTION

INFORMATION-SHARING ECOSYSTEMS: HOW THEY OPERATE AND WHAT THAT MEANS FOR PRIVACY LEGISLATION

Washington, D.C.

Thursday, June 27, 2019

Opening Remarks:

CAMERON F. KERRY
Ann R. and Andrew H. Tisch Distinguished Visiting Fellow, Center for Technology Innovation
The Brookings Institution

Panel 1: Information-Sharing in Different Contexts:

MOLLY ROBERTS, Moderator
Editorial Writer
The Washington Post

TREVOR HUGHES
President and Chief Executive Officer
International Association of Privacy Professionals

JAN SHAUGHNESSY
Senior Vice President, General Counsel and Secretary
Workday

LAUREN SMITH
Senior Policy Counsel
Future of Privacy Forum

AMIE STEPANOVICH
U.S. Policy Manager and Global Policy Counsel
Access Now

Panel 2: Marketing and Targeting: The Specific Cases of Advertising and Data Brokers:

STACEY GRAY, Moderator
Senior Policy Counsel
Future of Privacy Forum

JUSTIN BROOKMAN
Director, Consumer Privacy and Technology Policy
Consumers Report

PARTICIPANTS (CONT'D):

SHEILA COLCLASURE
Senior Vice President, Global Public Policy
LiveRamp

DANIEL A. SEPULVEDA
Vice President, Global Government Relations
Media Math

TIM SPARAPANI
Founder and Principal
SPQR Strategies

* * * * *

P R O C E E D I N G S

MR. KERRY: Good afternoon, I'm Cam Kerry and Andrew Tisch Distinguished Visiting Fellow here at the Brookings Institution part of the Governance Studies Program; and good afternoon; and welcome to #theprivacydebate. This is a project that we launched a few months ago, as some of you know -- I see a former partner of mine here -- I left a law firm where I was part time a few months ago to focus on the work at Brookings here and to use my role and the Brookings platform to advance the privacy debate. Privacy legislation is unfinished business for me from my time at the Commerce Department. I'm leading the consumer privacy bill of rights -- trying to put that in the form of a bill -- and I wanted to be able to engage in the debate.

I can tell you, a lot has changed since the time that I was working on that. You know, then, most Republicans and some Democrats were asking why do we need regulation. And saying if ain't broke, don't fix it. Now, we're hearing a broad consensus from really both sides of the aisle -- we need to regulate; we need to do something.

Back then, as we were working within the Department of Commerce on drafting legislation; looking for partners on the Hill to partner on the legislation and preparing a bill -- I couldn't find any. Now, we have members, you know, of all kinds introducing bills; committees conducting hearings; and lots of people putting down markers in this debate.

This has become a mainstream issue; and there is an opportunity now to get something done; and we need to act before that opportunity fades away -- before it becomes a wasting asset. And I will tell you that in these past months, I've been having a lot of conversations with stakeholders across the spectrum -- with trade associations; with privacy and consumer groups; and other civil society; with individual companies -- and I am struck by the opportunity that's there. Do not underestimate how many companies, genuinely, want to see some privacy rules in place; and it's not all about preemption. Sure, they want to see standards that would unify, you know, the privacy practices in the United States, but also across the world; and it wants a reason for consumers to trust them.

And I'm finding too that privacy advocates, consumer advocates, civil rights advocates understand this opportunity, and the opportunity to bring real protections to all Americans. So, I see a political will among stakeholders who are engaged in this issue; and, I think, the question now is whether there is the political will in Congress.

So, today's program is going to focus on a key issue in this debate. So much of this debate has been focused on social media and on big tech companies; but there's a lot more to privacy and data collection than that. These are really just a very large tip of an enormous iceberg.

We are in the midst of what I've described as a data big bang -- an expanding data universe that's driven not only by historically what we've had as expanding computing power, but now driven by network effects and expansion of networks; and devices everywhere connected all the time; and, you know, connectivity and bandwidth that are expanding the amount of data exponentially; and it cuts across all sectors and all spheres of activity.

So, all this data moves through various ecosystems; and the crux of this debate is what are the boundaries that we put on what's collected and what's shared in that process. These ecosystems have tremendous ability to expand the frontiers of human knowledge and efficiency, and the innovation in our economic system; but, obviously, tremendous implications for all of our privacy as the aggregation of information become more and more granular.

So, that's what today's panels are going to explore. It seems like this past week everywhere you look something is going on. There's some news in terms of how data is shared that's in the spotlight. Last week, the UK's information commissioner office issued a report that raised a serious question whether the ADTEC practice of real-time bidding enables advertisers to bid instantaneously to serve an ad to an individual -- whether that complies with European Union's general data protection regulation.

The Washington Post had a deeply reported story focused on the Chrome

browser and how browsing and cookies enable collection and sharing of data. We saw the Senate Commerce Committee, this week; and the Banking Committee earlier this month, exploring how data is collected and shared. During one of our panel calls to prepare for today, I said we really -- listening to our panelist -- we really could have a whole day's program on this issue; and, in fact, the Federal Trade Commission is doing exactly that today in its privacy conference; and we're fortunate Justin Brookman, one of the experts there, is part of our panel today.

So, I'm not going to introduce all of the panels. I will leave that to our excellent moderator. So, for the first panel, looking broadly at how data is collected; how it's used; how it's shared -- we have Molly Roberts, Editorial Writer for *The Washington Post*. She's on the editorial side, not the news side, but we'll still give her credit for that scene setting story in the *Post* last week.

And for our second panel, we have Stacey Gray who is Senior Policy Counsel at the Future of Privacy Forum, a think tank, and leads the ADTEC working group of FPF -- really tries to keep its members and associates abreast of what's going on in ADTEC. It's a continuing moving process.

And we have a terrific group of panelist who bring broad perspective, both on the technology, on the systems, as well as on the policy issues. I want to acknowledge and grateful to Workday that is represented here by Jim Shaughnessy for its support of Brookings' independent scholarship.

So, please -- silence your cellphone, but, you know, feel free to use it with the hashtag -- well, it has to have data collection -- it should say #theprivacydebate -- you can use either one.

So, the challenge that I want to put to panelist today; and, ultimately, to legislators is this -- in a democratic society, we believe in the value of information; and the flow of information; and the advancement of human knowledge. And as individuals, we are motivated to share, as part of how we interact with people; as part of the activities in the

world around us -- whether it's connecting with community to buy products; to protect the security of our devices or our information; to get free services; or to express views on the issues of the day.

But we want to be assured that the information we share for these purposes is going to be used in ways that are consistent with our expectations, our interests. And too often we don't have good enough reason for this assurance. And that's especially a challenge in the areas that is subject of the second panel. Data is like water, it flows; and it leaks. And we see that in ADTEC, some of those real time bidding systems may be designed to serve ads without using names or other identifiers without disclosing that identifying information, but that there's the ability to retain information and to correlate it with other information to build profiles. The ICO in England found that a single visit to a site can generate hundreds of contacts and circulate information to hundreds of organizations.

And as new developments -- cookie controls; ad blockers; ad IDs -- come into play, in order to protect privacy, somebody manages to design around them. So, we are, in effect, in an arms race in ADTEC. And the only way I think we are going to deal with that is with a set of ground rules that create a set of rules that everybody has to play by, and that punishes those who break the rules.

So, the crux of that debate is rules on collection, on use, on retention and sharing of data. That's what's going to change the system that we have today for most of the data that's collected. And certainly not to double-down on the existing system by treating data as property and, simply, substituting negotiation fatigue for click fatigue as we have today, and as John Morris and I have written in a tech tank blogpost, out today.

So, legislation won't be able to address all of the contingencies, but it can address developments with broad enough enforcement powers and tools like rulemaking and enforceable codes of conduct.

So, I raised the question at the outset whether there's the political will on Capitol Hill; and I would say, you know, we have been seeing an unusual effort to legislate in

the classic sense -- to learn the issues; to build the coalition; to work on a bipartisan basis; to reach out to stakeholders. But we need to seize this moment before the default to polarization and partisanship takes whole; before people become hardened in their positions; before more states step in and preemption becomes more intractable; before people decide that privacy legislation is just too hard.

So, Shakespeare wrote that there is a tide in the affairs of men -- and I would add women -- which taken at the flood, leads onto fortune. Omitted all the voyage of their life is bound in shallows and miseries. On such a full sea are we now afloat, and we must take the current when it serves or lose our ventures. So, I think, Shakespeare must have been thinking about baseline privacy of legislation (laughter) when he wrote that.

We're on a full sea today, and we must need to take the current when it serves or lose our ventures. So, thank you very much; and ladies and gentlemen, I give you our first panel, and Molly Roberts. (Applause)

MS. ROBERTS: Great. So, as Cam said, I'm Molly Roberts. I'm an editorial writer at *The Washington Post* covering technology in society. So, that involves a lot of things, but it has also involved, especially this year, data privacy. So, I'm really excited to be here and to talk to people who have been doing a lot of work and a lot of thinking in that area.

Also, like Cam said, when we talk about data privacy, we usually think about social media, targeted advertising, marketing; and you guys will get a chance in the second panel to hear a ton about all of that. We also are mostly thinking about those things when we talk about what the writer Shoshana Zuboff calls surveillance capitalism. She defines that as a new economic order that claims human experience as free raw material for hidden commercial practices of extraction, prediction, and sales. Big data is, obviously, much bigger than social media and the ways that information is shared for public and private interests are vast, they're varied. They go from the Internet of things in smart cities, to research, to health monitoring, and beyond. These information ecosystems -- which is what

we're calling them here -- obviously, come with benefits, and they come with costs, and any privacy legislation that we hope is forthcoming, will necessarily mean some tradeoffs between the two, which is what we're here to talk about today.

So, we have here to talk about that, Trevor Hughes who is the President and CEO of the International Association of Privacy Professionals. We have Amie Stepanovich who is the U.S. Policy Manager and Global Policy Counsel at Access Now, an international nonprofit that advocates for a free and open Internet.

We have Jim Shaughnessy who is General Counsel at Workday which offers human resources and management software to workplaces, including mine. And we have Lauren Smith who is Senior Counsel at the Future of Privacy Forum where she focuses on big data and the Internet of things, especially as it relates to connective cars.

So, we thought that since it's a broad topic, it would be useful to start pretty broad and get an overview from everyone on our panel, starting with Trevor who really has that whole expanding universe of data under his umbrella; and Amie as well even on that broader level; and then maybe more specifically in the context of what they're working on, Jim and Lauren. So, if you want to take it away, Trevor.

MR. HUGHES: Great. Thanks, Molly; and thanks to Cam and Brookings. This is a wonderful gathering and an important conversation. My name is Trevor Hughes, and I lead the IAPP, the International Association of Privacy Professionals. We are a not-for-profit organization based in Portsmouth, New Hampshire; and we are the professional association for people who work in this emerging field of data protection and privacy around the world. We have 51,000 members in 120 countries; and, currently, we are adding over 1,000 members a month. So, something is happening -- something is happening out there in the world. This issue of data protection is driving behavior not only in the marketplace but also in the public sector. We see both governmental and private sector privacy professionals flocking to the IAPP. Our conferences are full; our certifications are growing and expanding around the world.

I thought today that I would offer a bit of perspective of the growth of the profession and then come back to how I think that may actually speak to some of the policy issues that we're facing. Before I do that, let me just mention that the IAPP is policy neutral. We're not an advocacy organization. We intentionally like being a big tent; we like to say that we don't take sides in the fight, but we really like the fight. And so, all of the combatants, we welcome them to our big tent. So, anything that sounds like an opinion is probably mine and shouldn't be attributed to the IAPP.

The privacy profession is relatively new. The IAPP was formed in 2000. Some of our earliest members are actually here in the room with us today; and it has grown significantly since 2000. But in the last two years, we've doubled in size. I mentioned we have 51,000 members; just 2 years ago we had 25,000 members. So, something really significant happened in the last 2 years; and, I think, it's fair to say that the acronym behind that happening was GDPR. The General Data Protection Regulation in Europe drove significant activity for the IAPP. We have 26,000 members here in the U.S.; 16,000 members in Europe; and so, we have more members in the U.S. than we do in Europe even though it is the GDPR that has really driven much of the activity.

In fact, our European certification is our largest selling certification here in the United States. And so, one of the things that I think is really notable is that these policy developments like GDPR -- and, actually, we can look back to 2003, and SB-1386 in California -- the first data breach notification law -- that really drove a pop in IAPP membership. These policy developments have consequences in the private sector. Organizations understand and access the compliance risk, and they respond to it.

Interestingly, because of the extra territorial nature of the GDPR, the U.S. and the rest of the world is actually responding to this European policy initiative in a very significant way. And I don't want to overstate this, but I think it is fair to say that in terms of influence around organizational behavior with regards to data around the world today, the GDPR is the guiding principle. In fact, our European certification is our largest certification in

every region of the world -- Asia, Australia, New Zealand, Latin America, here in the U.S., and certainly in Europe.

I also want to mention that the growth of the profession, the growth of the operationalization of privacy has also occurred absent policy initiatives. So, prior to GDPR, here in the United States, we had many thousands of members, and that was in the absence of a broad-based policy initiative, a broad-based privacy law here in the United States. I think that's because the complexity and risk associated with data in society has been on an ascendant path; and that complexity and risk, when organizations look at it, they respond to it by using the best tools that they possibly can. And in the absence of clear guidance from public policy, they revert back to smart people in the right places making good decisions for their organization. They revert back to professional judgment, business practice, and risk management inside their organizations.

And so, even without public policy initiatives, we have seen the rise of the profession of privacy which I actually think is one of the interesting and less documented realities of the new digital economy. That the profession has emerged -- the risk management tools, the business practices of managing data inside organizations -- have really emerged in the absence sometimes of public policy initiatives. Deirdre Mulligan and Ken Bamberger wrote about this really well and thoughtfully, I think, in Privacy on the Ground, a book that I recommend to all of you.

I think we are in a special moment though; and Cam captured that poetically with Shakespeare. I think we are moving out of the Allen Weston era of thinking about control as the primary mechanism in which we manage data, and into a more complex and fragmented set of tools that includes public policy, but public policy that drives particular behaviors.

I think it's notable in GDPR that there are tools within GDPR that move beyond control and towards accountability and also towards user empowerment -- towards data subject empowerment. Requirements around accountability so that you know what

data you have; you know how you're using it; and you know you can report out on that; but also that a data subject can come to you and say, show me my data. They can also say delete my data, or give me my data. Those are really powerful tools, and they are different from a prior era of public policy responses which largely wrapped around notice and choice. And, I think, that gives us an indication that we are headed towards more of an accountability and stewardship model with regards to data. With some, I think, legacy notice and choice controls are still in our public policy.

With that, I'll pass things on; but, I think, it is an exciting moment for us; and I just want to note for the room that one of the things to watch is not so much -- yes, watch the public policy debate, and absolutely I'm glued to the news every day because there's something happening in our field -- but look at what the operational response is inside organizations, public and private, around the world because that's where you're actually going to see how organizations are dealing with the risk and complexity that they are facing; and it's been a pretty remarkable response. I have 51,000 members who are part of that response; and, I think, it's a big part of the story.

MS. ROBERTS: Great; and Amie.

MS. STEPANOVICH: Sure. So, we're going to hear, I think today -- and we hear in life almost -- a lot about the benefits of technology and the collection of data; and the way that it drives forward society in really positive ways; provides positive benefits -- and because I often get told that I am a pessimist in this field, I do want to start off by recognizing I think tech is really cool. I have read and watched Syfy since I was really young and my parents introduced me to Star Trek and Star Wars, and I thought that is really neat; and the fact that the technology that I was seeing then is now far surpassed by the object that I carry in my pocket, and this thing I have on my lap. That's fascinating; and so, we're in a moment right now. And somebody said to me recently, we're going to be really -- the people in this room -- one of the last generations that remember what it's like before that was the case. And who has some idea of the pre-technology world in order to judge how this is impacting

our lives.

And so, where I want to go is yes, it's really cool, and I want that tech future; I want to build it; I want to see where we can go. But it comes with so many risks attached to it; and to really kind of tease out those risks -- because if we don't plan for them; if we don't protect the most marginalized people in our communities, then we're going to stray away from the future that could be into one of those dystopias that we see in movies, and have for the last few decades.

So, there are four points I want to make to start off; and then kind of get into the discussion; and I hope to move pretty fast. One is that there are a lot of layers to data collection; and so, we like to think about data as the post that we put on social media, or the information that we turn over to certain companies when we sign up -- our name, our address, our phone number -- and that's all really important, but it's really only the surface layer of this ecosystem that we're talking about. And underneath that is the information that's picked up just by virtue of our existence -- when we walk around in the world; when we carry our phones; when our location is tracked; information that is picked up by inference. When we sign into certain services, there are implications about when you're using those services; when do you eat meals in the evenings; and when are you ordering delivery. That can lead to certain types of implications that get put into profiles about you, and cause for certain decisions and determinations to be made.

And then when we get into smart cities, connected cars, connected workplaces -- to talk about two of the things that we're going to go into more detail -- that collection gets a lot bigger. And so, it could be our conversations walking up and down the street picked up by a smart light post, which was something that I was researching in my career eight years ago. You know, you think about these things as new technologies but they've been around for a while and they're being deployed. It could be what is going on in our bedrooms, or what our children are doing during connected toys that are now collecting all sorts of information. This world is very large, and we have to be thinking not only about

that surface layer, but all the way down the stack.

The second thing is choice. So, when you get away from that top layer -- and I would argue that we really don't have much of a choice about that top layer either, if we want to participate in society -- but as we go further down, choice seems to look like less of a solution. When you're interacting through voice technologies; when you have these different interfaces, you can't necessarily opt-out to the extent that you could choose not to use Facebook, for example -- something that a lot of people use, as an example, for me today -- and so, if we focus around choice -- I think, that's a theme that we've already heard today through Cam's opening remarks; through what Trevor said -- we're losing part of the conversation; and so, I'm getting way pass that in order to address all of that other collection -- and the threats that are both seen and unseen.

There are real worries that, I think, people have about the data that is collected about them, and how that can be used; and there's the overt threats -- for some people, it's I'm getting served an advertisement that I don't want to see -- I don't know if I, necessarily, see that as a threat, but some people do; and I take that to be legitimate. All the way down to I'm having my information turned over to police and it's being used to track and monitor my movements, which, I think, we see as a much more legitimate reason and thing to worry about -- and that's just my basic data collection.

When you move deeper, and we talk about manipulation of people's activities and habits and the way we think, that's kind of where the future of technology is going. It's getting into a place where we're getting suddenly nudged in certain directions by companies because of the data they're collecting about us in the profiles that are being built; and those threats are really seen by certain communities.

And so, I'll end by talking about some of the communities that I think both really benefit from technologies, but are going to have more threats placed on them because of that -- and I'll call out two. One is going to be the LGBTQ+ communities. It is unquestionable that these communities have benefited from being able to connect through

social media; from being able to share their stories; from being able to have support networks in places where they may not have ever had before; and that's been a tangible benefit to some of those communities through technologies.

It is also unquestionable that they have faced arrest -- sometimes worse than arrest, torture, imprisonment, etc. -- because of data that have been connected through these platforms. Some people have been ostracized; there are people who have been outed. There was the situation at the Olympics not too long ago where reporters were trying to identify LGBTQ members in the Olympic population through their use of applications like Grinder, and they were getting on there to try to figure out who those people were. And so, seeing the benefits and then the threats that are faced, we want to emphasize the benefits while really preparing and putting in the protections we need to make sure those threats are limited however possible.

The second one is the accessibility community; and, I think, this is where we see it even more pronounced. There are people who are blind, who can't hear, who can't walk, can't really get around. Technology has helped them interact with society in a way they probably never could have before. To describe what is being put in front of them; to go out and move around and be more mobile than they could have previously; and so, it's provided a lot of benefits. But when a piece of tech can see every single thing that you're interacting with throughout the day, and collect information about you, or hear every conversation that you have; and the purpose for the technology is to collect that information; to be able to provide the benefit; and to create those profiles; and to make sure that they're serving those populations, those come at great risk for long-term marginalization and further detriment to the communities.

And so, what we're looking for is to measure the potential threats for those communities; look at the solutions in the form of potentially U.S. federal legislation, state legislation, laws in other places around the world, and make sure we're accounting for the threats that those communities could face and that we're going to be protecting them in the

long run. So, that's my pessimistic take before we get into the other cool things that's going on. Sure, yeah, a little more optimism in the cloud computing context.

MR. SHAUGHNESSY: That puts a lot of pressure on. I don't tend to be that cheerful about a different view of the future. But thanks for that opportunity.

MR. SHAUGHNESSY: And thanks to Brookings for putting this event on, and, particularly, to Cam for organizing it and bringing us all together. And I also would like to commend Cam and John Morris. I read the blog that was posted yesterday -- and this is a subject about which I spent a lot of time thinking, and thought my thinking was pretty advanced; and I read that blog and thought well, there are a number of things that I was probably not thinking about the right way -- and so, we'll change a lot of what we do. So, I really commend it to everyone who's here to find -- I imagine it's pretty easy to find online now -- and read it because it's really quite insightful.

MR. SHAUGHNESSY: So, I'm here to talk about this -- the privacy debate -- from a different perspective that most people think about when they think about privacy -- and that is, the perspective of enterprise cloud companies, of which we're one.

So, first is a rhetorical question, and you can raise your hand or not; but I assume that many people here took Uber or Lyft to get over here today -- me too. If you got a text message from whichever service you used -- that seemed to be from the driver -- you were, actually, interacting with an enterprise cloud company; and it's a Twilio system which provides the backbone for all of that. And I don't know if anyone -- daily, today, people are probably thinking about getting out of Washington for the summer; it's kind of hot; get some place cooler -- if you made your arrangements through Airbnb -- probably a few people have done that as well -- and you've interacted with customer service, you probably interacted with another enterprise cloud company, and that is SanDisk who provides that level of service.

We provide a different level, different type of enterprise cloud service. We provide human capital management, financial management, and analytics and planning

solutions to large enterprises, including government organizations. We're a young company -- only 15 years -- but we've been blessed with a lot of success and great growth. Enough that we now count 50 percent of the Fortune 50 and 40 percent of the Fortune 500 as our customers, including *The Washington Post*; and hopefully organizations you all work for, or if not, we can make an arrangement for the future.

As part of that, we've been entrusted with the records of about 39 million employees of those companies, and many more -- non-employees, including dependents of the employees, as well as former employees. And it's interesting how that works because every employer for which I've worked since 1988 -- which is longer than many of the people in the room were born -- but now uses Workday. And so, I may have my records in Workday in multiple different locations, but Workday wouldn't know that as it turns out.

What we do is -- like other enterprise cloud companies, we have a different relationship today than our social media counterparts. We don't monetize the data. We get paid by subscriptions from our customers, and they pay us well, thankfully; and we help customers make better use of their data. (Inaudible) trust us through highly-functional software, including for us, applications and features that are enriched by machine-learning algorithms, and other technologies. But it's all about helping customers make better use of the data.

So, for us, it's helping customers recruit the right people; it's helping them hire and bring them on board; it's helping with their development and their training; it's helping them pay them -- hopefully, the right amount and on time, because that's generally appreciated -- and then help also delivering benefits. So, another way of thinking about this is we don't really make decisions about the data. Those are made by our customers who control the data, and we just do what we're told as we process the data.

And our business depends, like the other enterprise cloud companies, on a high degree of trust with our customers; and they have to have similar levels of trust with their customers, or else the system doesn't work. And it turns out that we all operate in

information-sharing ecosystems that are already pretty highly regulated, so. We've talked a bit about GDPR. GDPR is a regulation that impacts the information-sharing ecosystems in which we operate; but it's also a function of employment law; payroll law; tax law; benefits law; HIPAA, and a variety of other regulations that apply to these specific contexts.

But despite this, the existing regulatory framework, which actually provides more protection than people generally recognize, we are one of the companies to which Cam referred, who are supportive of strong federal privacy legislature. We believe that it's important, one, to establish trust; and it's important, two, to ensure interoperability among regimes operating around the world. And GDPR is the leading regime now, and it does influence behavior all over the world; and also to achieve consistency in treatment in the United States.

And I'm fortunate to be a resident of California where I will receive protection under a landmark state statute that was passed within the last year, and goes into effect next year. But I don't like -- I would, as an individual I much prefer the protection of a strong piece of federal legislation that would ensure that I'm protected wherever I happen to be, and dropped data wherever it happens just to show up in the United States, and would provide the inoperability that we've talked about in the past.

We think that the federal legislation, like GDPR, should be based on the OECD fair information principles. We believe in strong enforcement by the FTC and also by state attorney generals, as appropriate; and we'd love to see them have the power and the resources necessary to enforce. And also believe that it's really important that the legislation be nuanced to recognize the operation of different information-sharing ecosystems' different characteristics and, particularly, how those obligations would likely differ for controllers and processors, just like in GDPR.

MS. ROBERTS: Great; and, finally, Lauren.

MS. SMITH: Great; I'll try to bring some optimism as well. So, you may be surprised to see a focus during a panel talking about privacy more broadly, to have a

conversation focused on connected cars and mobility technologies. But this is actually a really fascinating space from the perspective of privacy right now because it's a space where you can see very clearly some of the benefits of advanced technologies and sensors to literally save lives. But you also see a space that is at the very early stages of the creation of a data ecosystem, and there's a lot of promise there; but, I think, this sector can learn a lot from lessons that have been learned in other areas -- like we'll hear about ADTEC. And there's a lot of possibility if privacy is taken sort of seriously from the outcome -- there's a lot of promise from the safety perspective.

So, to level set a little bit, data collection in cars is not entirely new. There've been computerized systems in vehicles since the 60s, and there are a couple that are in nearly every car today. One is the event data recorder which is the black box of your car that records information related to a crash, or a near crash event; and the other is the onboard diagnostic system which is what sets off your check engine light, and allows you to go into a repair shop and they can look up with a code to understand what's going on, on a given car.

But despite those being in cars for a long time, there're some significant new developments in this space. When I go to transportation conferences, the sort of takeaway message is that the transportation space is going to change more in the next 5 years than it has in the last 50. So, there's a very rapidly changing, sort of change-or-die, adapt-or-die perspective in this market right now; and a lot of that transition is including looking to data to see are there new technologies that we can incorporate, such as autonomous vehicles, as well as are there market opportunities to use and monetize this data in a way that will be essential to being a part of this ecosystem going forward.

So, as these technologies are integrated, cars become more and more like computers than these kinds of mechanical chassis that we're use to that used to sort of safeguard our autonomy and freedom. They've become, essentially, another item in the Internet of things; but it's actually not just one item. When you get into a vehicle, there may

be a number of IOT technologies inside. So, questions that are being raised around biometrics; questions around microphones; always-on-technologies; ISPs; video screens; web browsing -- all of that can actually happen within a single vehicle.

There's significant growth in this space. So, some estimate that 286 million in connected cars will be added to the market in the next 5 years. So, I think it's going to be hard in five years to actually find a car that doesn't have some sort of connected technology.

So, the good news is that the sensors that are powered by this data have the ability to transform safety and convenience on the roads. Right now, the statistics for car crashes in the U.S. are very grim. We've sort have become desensitized to them; but 37,000 people die in car crashes every year here, and human error is a factor in 94 percent of those crashes. So, a lot of the new technologies in this space are being developed to help mitigate some of that human error.

So, one way of looking at it is your car is learning more about you, but what it learns may save your life. I'll give you a couple examples of some of these technologies. There are external sensors that are analyzing the environment and reacting within the car, as well as internal notification and convenience features. One example is automatic emergency breaking which uses camera or radar-based sensors on the front of the car to break automatically if it detects that an accident is about to happen and the driver hasn't braked in time.

Eye-tracking technologies can track whether a driver is paying attention to the road, and send notifications if they're falling asleep. There's also advanced versions of that now that try to do health monitoring to tell if someone is having a health incident and can pull the vehicle over. Vehicle-to-vehicle communication enables the sending of messages between nearby vehicles that can send location, braking status, and heading. So, if a car in the front needs to break suddenly, it can communicate that message several cars back to help avoid a pile up.

This technology was estimated by the Department of Transportation to,

potentially, address up to 80 percent of multi-vehicle crashes; and there was actually a lot of work done to create a federal mandate that would require vehicle-to-vehicle communication in all new cars; and it would be mandatory, no opt-out available. That is not currently going forward, but it was proposed during the Obama administration; and there's definitely going to be versions of this technology incorporated going forward. The debates are on the band of spectrum and not about the use of the technology.

So, at the same time, the volume of data has significantly increased -- both the data that is generated and collected, as well as shared off the vehicle. So, the Intel CEO has said that one autonomous vehicle will use up to 4,000 gigabytes of data per day. Others have said AVs being tested could generate up to 1 gigabyte per second. So, we're talking large quantities of data. For AVs, in particular, this enables the machine-learning process to sort of analyze and learn from prior incidents; and, hopefully, prevent future accidents. But, even on your way up to autonomous with more and more connected cars, they're more and more devices.

Some of these come built into the cars; some can be added on. You may be getting advertisements from your insurer that you can plug in a device to your OBD port and get a safe-driving discount because they'll analyze your driving behavior and, supposedly, determine if you're a safe driver or not. So, it's something where, you know, you may own a foreign car, but you may buy a Verizon (inaudible). There're a couple of different entities there. There's also syncing between phones and cars, which is not always done in the most notice and consent friendly way.

Another big change is the air gap that used to exist where you needed to go to a repair shop and have them plug into your OBD-II port to read the codes; now that air gap is gone; and, increasingly, information is being sent off of the car. A range of technologies are leveraging that connectivity for services; and that information can be transmitted in a variety of ways; and is collected by a growing variety of parties.

So, this is sort of a new space, and the types of data involved range from

sensitive, privacy relevant types of information to less so. So, when you're dealing with, say infotainment and personal communication data that could include your contacts lists; that could include phone conversations that you're having when you're in a vehicle. Then there's sort of less sensitive data, but that may be linked to your individual car, like vehicle health and operational information.

Just like any other technology, there are conveniences that users may be interested in. There are partnerships like Warner Brothers and Intel partnering to be able to show video content in autonomous vehicles, which you can imagine consumers enjoying being entertained while they're in a car without needing to steer or drive. There will probably be commercial breaks. There is, increasingly, you're seeing GM has a marketplace option where you can get advertisements for discounts on nearby stores.

So, there's a lot of unresolved questions in this space -- who gets the data; who manages the consumer relationship; and what information is personal. Again, we're in early stages; and the data flows are not exactly clear. So, the data may go directly to your manufacturer that you know who that manufacturer is because you bought a car that has a symbol on the front; but in the automotive space, there may get suppliers involved. You may be in a ride-sharing vehicle; so the ride-sharing platform may have information.

The services that you sign up for -- subscription-based services in the car -- that information may go directly to the company that you signed up for -- they may not actually go through the manufacturer. So, that's going to wind up being a big consideration when it comes with sort of complying with some of these new laws and thinking about how to regulate the space, is that the data flows do not necessarily go through the entity that the consumer has the direct relationship with. I think that can raise a lot of questions when it gets down to notice access consent.

There's growing methods of modernization, as I mentioned. There's a small number of connected car data marketplaces that are just beginning to navigate the space. This is seen as a potential, very large market. McKenzie estimated that money from car

data modernization could be worth as much as $750 billion by 2030. So, there're a lot of opportunities there, and we'll sort of see different folks experimenting with how to make the most of that.

Automakers -- proactively thought -- saw this issue coming and they created a set of privacy principles in 2014 that nearly all of them signed on to -- which is a great first step -- modelled mostly on the Phipps. There are a couple major commitments around transparencies, having the privacy policies are on affirmative consent for sensitive data. Things like biometric behavioral location data, as well as limited sharing with government and law enforcement. So, compliance with those, I think, gets folks along the path towards being compliance with other privacy laws.

That said, this sector is, again, very new and growing; and there are a lot of dynamics around access to this information; and folks are in different spaces from automakers, to ridesharing, to repair shops, to rental cars are just starting to navigate what data they have access to; who owns and controls that data; and, I think, we're seeing that play out in some of the conversations around privacy regulation where folks are seeking carve-outs for safety data; but there're also underlying questions around who in this space has access to which data; and those will be important going forward.

MS. ROBERTS: Well, thank you guys all so much. We have a lot more to work with than we do time; but we will do our best and also do our best to leave time for some audience questions. I think the best place to start might be the question of notice and choice, or notice and consent. It is definitely a thread that I heard running through this. So, I wonder if we can begin, Amie, with you saying a little bit about there's this feeling that notice and choice is not enough. If it's not enough what makes sense to go on top of that?

We've heard about obligations on the companies holding the data that are kind of broad. We've heard terms like duty of care, and duty of loyalty thrown out there. We've also heard about more explicit use limitations. I'm curious from your point of view what sorts of things are necessary; what would work well?

MS. STEPANOVICH: Sure; and I think, Trevor said a really important word -- actually, he said many important words. He started by saying we have to move away from a framework around control and move toward one of empowerment and accountability. And, I think, empowerment and accountability is right. But I would almost say we never really had a framework about control because there wasn't really -- without the empowerment and the accountability, that control element was never really there; and so, I guess I would answer your question with three things amongst many other items that we would like to see.

One is those use limitations. We think that data should only be collected or used if it falls into one of a certain enumerated set of categories -- and this is straight out of the GDPR. Consent was one of those; but you could argue -- and many do -- that consent in the GDPR is not even the best basis for collecting information. The GDPR also has legitimate interest of the business, and our take is that probably is a bit too broad, actually, from a human rights perspective, and it needs to be narrowed down in a way that is more meaningful because legitimate interests of a business can be interpreted very, very broadly. So, that's the first set of things.

The second is actual, actionable user rights. And, I think, this is a -- two years ago I couldn't have said this -- but at this point a pretty non-controversial aspect of what we're looking for in federal privacy law. You should have the ability to access the data that an entity has about you; to port that data somewhere else; to delete it if it's no longer going to be used by you, if you want to leave a service. Now those rights shouldn't, necessarily, all apply to the same categories of data; and that's going to be really important when you talk about all the different types of data going in.

If I go to a company and ask them to exercise my right of access, I want to know everything they know about me. I want to know what they have; the inferences they're making; the whole cha-bang. Now, I don't necessarily think I should be able to erase all of that data. There are a lot of genuine reasons: for legal purposes; if it's a photo that I happen to be in but somebody else took it and is responsible for it; that may be shouldn't be

something I have the power to cause them to erase.

Same with portability -- not everything, necessarily, should be ported over. There are other privacy concerns that, actually, could be implicated in that. So, we're going to have to determine what rights apply to what types of information, and that needs to be pretty granular.

And then the third thing is this morph's category of creative stuff that we've kind of been trying to think out about what should be in a federal privacy law to protect people; and one thing in that amorphous bucket of creative stuff is we have looked at federal benefits -- either in the form of grants, or tax breaks, or incentives for contracts -- to companies that explore business models that aren't based on data. And so, if we can get away from that type of business model -- it's not going to be necessary; we don't want to compel it -- but to provide incentives to explore and to like gen-out those creativity juices for business entities to get away from driving their business models based on data, and look at other ways and other things that can take place -- and so, just a few things that we would throw out there.

MS. ROBERTS: And, Trevor, I know that your organization doesn't take policy positions, but I'm curious about your take on the notice and choice question too; and maybe how some of your companies are thinking about, particularly in the context of GDPR, fulfilling their obligations on top of it.

MR. HUGHES: Sure. So, first the IAPP has members across both public and the private sector; so it's not just companies. I think our members are struggling with notice and choice as a non-scalable method to respond to many of the challenges that they see in the marketplace today; and when I think about notice and choice -- just from my own perspective, having been in the field for a fair bit of time -- we've been critiquing notice and choice for a long, long time. Fred Cate, almost 20 years ago, wrote about the failure of the fair information practices; and more recently Woody Hartzog has offered a really strong critique of consent as a mechanism. I think it is fair to say that these analog public policy

tools are not working well in our current digital economy -- they really are not working well.

Here's a great example that we haven't talked about yet on the panel that, I think, demonstrates the tension of choice in a broad, technologically driven, digital economy, and that is around genetic privacy. If I take a genetic test, I learn genetic information about myself, but at the exact same time I am creating, disclosing, learning genetic information about many of my family members; and we are actually seeing a whole new realm of genetic surprise emerge where things like artificial insemination, unknown parentage, and many other things are emerging from these multiple genetic tests.

Now, there is no industry that layers in more consent than the genetic testing industry. I did an Ancestry.com genetic test because I'm a genealogy buff and loves researching my family history; and I was a student of the consent process that I went through -- and trust me, it was robust. But my parents -- my brothers, my aunts and uncles, my cousins -- none of them had any involvement in that process, and yet their data was implicated in that test. Consent doesn't work in that environment; and, I think, that's just one example that we could take out to the broader digital economy and just show that the complex data ecosystem which we currently operate within really doesn't allow for notice and choice to be complete solutions. I don't want to give up on them totally. I think there are moments -- and I liked Amie's suggestion of layers of data collection and use -- and perhaps at top layers there are places where choice, where consent is a mechanism that makes sense. But, broadly, I think, there is a recognition that they are strained, at least, if not failing.

MS. ROBERTS: And, Jim, from your point of view at Workday when it comes to that controller, processor distinction that you talked about, how does something like notice and choice operate in that context and then how would a proposal -- you talked a lot about trust, like a duty of care, like the idea of third-party obligations then being extended to parties further down the line -- work for you?

MR. SHAUGHNESSY: So, fortunately, notice and choice is not a feature of

our relationship with our customers and data subjects; and by and large, given what our applications do, it isn't a big part of what -- we don't have an ADTEC application. And so, while we try hard to ensure that not only can our customers comply with all laws that are applicable to them when they're using our software, but they have multiple degrees of freedom in choosing how to comply -- notice and choice isn't a big part of that. So, I can opine on that, unburdened by any sort of practical impact or knowledge; but it seems like (inaudible) it seems not to be working with the mass collection of data; and, I think, that -- a sort of a corollary of what Cam and John talked about in the blog a little bit is -- the concept of ownership isn't very valuable, but understanding who has interest in particular items of data, including items of data that they may not be able to claim ownership of, but may still have privacy interests, it would be really valuable.

The concepts of duty of loyalty and duty of care are interesting. You know, in other areas of the law, they've taken a long time to evolve and a long time to decide exactly what they mean in a particular context; and so, expecting them to provide a lot of guidance in the short term -- if we were to apply those to a particular controller -- well, now you have duty of loyalty, duty of care -- it wouldn't make things a lot better in any foreseeable time period. It might make things better for our great grandchildren, or to grandchildren maybe, but not during our lifetimes.

MS. ROBERTS: I want to move on a little because I know Lauren you talked a bit about where notice and choice can fall short in cars, but I'm curious also about the question of any exemptions -- and I know that in the car industry there's been a little bit of advocating for exemptions for connected cars. I want to hear from all of you, ultimately, on that subject. What is the best way to look at -- maybe there're some companies that are dealing with certain types of data, or dealing with data in certain types of ways such that they should be treated differently. So, one way to approach would be these granular exemptions. Another way is something like a controller, processor distinction. Another way would be oh, if you don't monetize data, maybe we treat you differently. So, to start with you Lauren, just

in the car context and exemptions, I'm curious how you think that should operate?

MS. SMITH: Should operate; okay. I was going to tell you how it's currently operating.

MS. ROBERTS: Well, that works. You could start with that, and then we could hear whether you agree with how it's operating now, or want to change things.

MS. SMITH: No problem. So, yeah, actually in the past month or so, there's been some movement around efforts to treat car data a little differently under some of the proposed privacy laws. So, there's a couple in the works right now -- also, with the broadest one, which is in the Nevada privacy law, which is now long, in process. So, that law, actually, includes a very broad exemption for automakers, or payers, and servicers, which pretty much relates to all car data. So, this relates to any operator who collects, generates, records, or stores covered information retrieved from a car in connection with a technology or provided by a consumer in connection with a subscription or registration.

The argument that was made for this exemption as well as the others -- primarily around the ability to notify owners about recalls and safety, or warranty related defects -- and that sort of been the argument that has been used in each of these spaces. I think the Nevada one is quite broad, and so it might be a little shortsighted in terms of how this ecosystem is evolving to look more like these other data ecosystems.

California has -- there's an amendment to the CCPA that has passed out of assembly and into committee related to car data, but this one is much more narrow. So, it allows car dealers to retain and share vehicle information which is very limited. It's then make, model, year, mileage, and ownership information with the car's manufacturer specifically for the purpose of complying with warranty repair or recall. So, that one seems poised to go forward.

But there're some other efforts elsewhere as well around these questions have converged with kind of the right to repair copywrite issues that come up in the owner repair space sometimes. In Massachusetts, there's an effort -- I think advanced by the car

repair folks -- to ensure that the whole access to future platforms, and also trying to standardize telematics platform -- so, we'll see where that goes.

I think there's certainly, in some instances, a case to be made to treat vehicle safety data differently, particularly, you know, as I mentioned, DOT was considering mandating vehicle-to-vehicle communication, and the safety case is just very strong there. But I do think it's important to recognize that there are reasons why we are calling for a federal privacy law that would apply across sectors and ensure basic protections for consumers; and it's important to consider the space in that context.

MS. ROBERTS: Amie, your point of view on the topic of exemptions. I don't know if you have a broad-level opinion on it.

MS. STEPANOVICH: I think there might be a place for it. I hesitate to endorse any sector-wide approach; and, I think, we see some of that in the CCPA, and there are a lot of interests involved in getting some of those exemptions put into place. Some of what we see, actually, in the GDPR when it comes to exemptions -- when it's like certain categories of data or certain levels of processing -- that might be a better approach actually to look at and something that we'd be a little more supportive on.

One of the things and one of the related topics here is this distinction between sensitive and non-sensitive data; and if there're going to be different standards that apply, if something is "sensitive" -- and that is in the GDPR -- and we have in the U.S. conversations actually tried to get away from that distinction -- outright -- because when you start collecting, and collating, and combining databases, saying something is non-sensitive is really nonsensical because you're putting it with a lot of other types of data and being able to make a lot of sensitive inferences.

MS. ROBERTS: And, Jim and Trevor, I want to give you guys a chance to speak on this topic too before we move to audience questions, if you'd like to.

MR. SHAUGHNESSY: So, one thing I would say is that the controller, processor distinction is not really an exemption -- at least in our view -- it reflects the

different roles that the two types of people have in processing data; and as a processor, as I mentioned, like we don't know the names of our customer's employees; we don't know how much they get paid; we don't know what hours they work; we don't know what locations they work unless for some reason we're authorized to go in, in a support case, because something's not working; and that's probably better, right -- that we not know that.

And so, if we had the obligations of a controller -- a subject that come to us and say well, show me the data -- then we would have to be able to do that which is probably not consistent with what we're trying to accomplish.

MS. ROBERTS: Terrific. Then hand it over to the audience, and we'll try to get in as many questions as we have. I think we have about 12 or so minutes to do that. Do we have mics coming around? Great; so, yes, we'll start in the front row.

MR. BALKAM: Thanks, very much -- Stephen Balkam with the Family Online Safety Institute. Amie, you mentioned two populations right upfront -- the LGBTQ+ and the disability groups. Where do you think children and young people fall in this debate and, particularly, how well or otherwise is COPPA -- the Child Online Privacy Protection Act -- holding up after all these years, would you say?

MS. STEPANOVICH: So, I want to preface for this is not my area of expertise; but it's one of the populations that we think are, definitely, at greater risk of having their data manipulated and monetized, especially for longer periods of time. And, in certain circumstances, it's something that we've looked for greater protection, In that population we put it within -- Access Now focuses on "users at risk;" and people often asks me what that means -- and there's no definition -- it changes. I mean we work all over the world -- it changes in different countries; it changes at different times in different regions; and for the U.S., I would say children are definitely at risk. In certain circumstances -- in those circumstances we would want them to have more protection.

MS. ROBERTS: Yes; middle on this side.

SPEAKER: (Inaudible) the panel about the private right of action?

MS. ROBERTS: Sure; we can go down the line on private right of action unless there's someone who doesn't want to talk about private right of action (laughter); but we'll start with Lauren.

MS. SMITH: I think it's more a big-feet political issue. It's not one we get as engaged on; but, you know, I think, when it's an important when considering the political tenability of an ability to move forward on a law; and, I think, it's certainly a challenging one to incorporate right now at the federal level.

MR. HUGHES: I agree with her. (Laughter)

MS. STEPANOVICH: I'm going to paraphrase one of my colleagues, David Brody from the Lawyer's Committee, who often says marginalized communities have not been able to rely on institutions to protect their rights historically; and if we want to protect those communities, we need to provide them a private right of action. And, I know, Access Now, and several other privacy-oriented groups who do have a position, would probably -- would definitely -- pull support of a federal law if it did not include a private right action, and would never want to get to a conversation around preemption unless we saw private right of action first.

MR. HUGHES: A private cause of action is certainly one of the hottest issues with regards to public policy in privacy in the U.S., and also around the world. What I can say is that I have not seen a law or regulation that lacks significant enforcement capabilities work anywhere. So, the 1995 directive in the European Union lacked significant enforcement capabilities, and it has been written that massive non-compliance was the rule of the road in the European marketplace, including amongst many European organizations.

The GDPR, notably, has brought in fines that can go up to as much as four percent of global turnover; and that got the attention of many, many, many organizations around the world. I think the FTC has shown itself to have some significant enforcement capabilities; but even in those indicative, or sort of precedent common law of FTC enforcement-type cases, they can't even cover the whole waterfront.

The California AG came out in support of a broader private cause of action under CCPA because, I think, there was a recognition from AG Becerra that his office didn't have the enforcement capabilities, the bench strength, to really move forward. So, I don't really have a point of view, or certainly the IAPP doesn't, as to whether a private cause of action is the right answer. What I can tell you is that for accountability to work there has to be consequences in the marketplace for poor behavior. Whether those consequences are really effective enforcement by an empowered regulator or private causes of action in the courts, I think either could work; we just have to find the right mix.

MS. ROBERTS: Yes?

FEMALE SPEAKER: I'd love to hear thoughts on technologies that are potentially more ubiquitous, and people can't opt-out of, such as facial recognition software.

MS. STEPANOVICH: I'm on the World Economic Forum's Global Counsel On Consumption, and one of the things that we've been talking about over the last year is voice technology, which is the -- not, necessarily, a new technology, but a new interface that people are using -- and that different pieces of technology are building in; and, I think, that type of collection as you walk pass things is going to be quite broad, including in cars, and what level people who are passengers in cars, including Ubers and Lyft -- somebody brought up Ubers and Lyft -- are consenting to that type of collection. So, that's another one is voice biometrics -- beyond face -- is going to be a big deal.

It blows my mind, the technology that's being embedded into just infrastructure throughout communities and cities is going to lead to a huge, just increase, in passive collection of information.

MR. HUGHES: So, I'd love to respond, specifically, to facial recognition; and, I think, there are other technologies and innovations ahead of us that will similarly challenge our thinking about privacy. Something like facial recognition is going to fundamentally change the way we experience privacy in many context. And we don't, currently, have the tools -- I don't think -- from a public policy or an organizational risk

management perspective to address some of those changes. I'm going to reference Woody Hartzog again -- I'm a big fan of Woody Hartzog at Northeastern Law School. He's written about obscurity; and he is a very strong voice actually calling for a ban on facial recognition right now until we can get better controls in place. The idea of facial recognition where a picture taken in a public square can identify you even though you previously may have thought that you had the obscurity of the crowd as you were walking through that space, that changes the context of privacy as we experience those spaces. Those contextual disruptions, those changes to the context of privacy, are really, really challenging; and this goes beyond a strict data-driven type of privacy analysis that we've had to date. I think facial recognition is one example of that. Just to wrap this point up -- we're in the middle of strategic planning at the IAPP. We've just gone through two years where we've doubled in size, and we are projecting continued growth. And as we look at issues like this, we actually see lots of growth in the years ahead for the IAPP because of the complexity and the challenge of these issues.

We don't have easy solutions for them right now, and there's tons and tons of work to do for us to figure out the privacy structures that we need to put in place to manage this.

MS. SMITH: And I can just add another example from the car context, not just inside of cars, but increasingly, autonomous vehicles, as they are understanding the spaces in which they are operating, there is, essentially, sort of a mapping war to be able to create high-definition maps that are sufficiently detailed and accurate to be able to provide the baseline for autonomous vehicle's ability to navigate; and a lot of that will wind up involving externally facing video, as well as lighter and other sensors don't reveal as personal information. So, in some of these testing areas, there are cars driving around constantly, daily in the same neighborhoods with video constantly going. And, I, personally, have a lot of questions around, you know, that may be a space where we should come up with some privacy principles upfront around retention; around whether they should have the

ability to, you know, use facial recognition within these databases.

I think, right now, they don't plan to; but there's also a use case for not, say, blurring faces or license plates because some of the engineers argue that if you can't see where a pedestrian's eyes are pointed when they're crossing in a crosswalk, you can't tell whether they are looking up and seeing the vehicle and getting the signal to stop, or if they're looking down at their phone. And so, that it can be important to keep faces in that kind of database, at least initially. So, I think this technology is going have to grapple with that and, you know, questions around how you deal with some of these privacy projections where you're dealing with passersby or neighbors who did not sign up for the service and may not even be aware that their life is being included in a large data set that a private company has.

MS. ROBERTS: Okay. I think we have time for one more -- and I see two more. All right, we can try to do two more with very quick answers. Yes; please; go ahead.

SPEAKER: Thank you for your time. I wonder how the panelists anticipate we're going to be able to deal with the inferences that are being made about the data because the data doesn't belong to the one individual person, but is part of the pattern recognition that empowers the larger sphere of knowledge that's being developed.

MS. ROBERTS: Sure. Does anybody want to speak to inferences?

MS. STEPANOVICH: There've been really great conversations about societal -- like the interests society has in privacy -- and, I think, it's going to continue to be a part of the federal privacy legislation. And as to you hinted at ownership again; so, I'm going to point us back to Cam's really great blogpost that went up today about ownership because I'm really hoping we can stop talking about ownership of data. I think it lead's itself to predatory practices.

MR. HUGHES: Just a quick comment. I think there's a lot of social ambivalence. So the well-publicized case a few months ago where a serial rapist who debated detection and capture for 30 years has been caught because of this use of -- his

relative had posted genetic information to a social site, and they were able to match the DNA evidence and focus on him as a suspect. Even those of us who fear a dystopian future cheered that this guy got it, right. Like it was time, and that we have more faith in DNA evidence than we should -- someone will tell me that I'm wrong.

But then there are other times when, you know, we hear other things where people's lives are jarred by hearing about an unknown sibling or hearing that the person that he or she may have thought was a parent was not a parent; and so, I think, there's a lot of ambivalence and we haven't sorted it out yet. I don't know if privacy law with a vehicle will do that; we'll find out.

MS. ROBERTS: And, we'll do one more; yes; thank you.

MR. ROTH: Thank you -- Alan Roth from Sidley Austin. If we were doing this panel in Europe, Brussels certainly, someone would have introduced the notion or concept of ethics -- ethics as a form of self-governance; and, therefore, accountability that is brought about kind of internal to an organization. Do you all think that there is a necessary role for ethics as kind of a, you know, digital governance within company's organizations, especially as the data processing techniques are increasingly opaque and barely understood by the scientists involved; and certainly not by leadership who are not technologists. So, do we need to evolve standards of ethics which are then inculcated through kind of a culture of ethics in compliance as a means of establishing, you know, self-accountability -- if you will -- which could be I'm sure somehow enforced externally, as well. But what do you think about that notion?

MR. HUGHES: So, I'm a strong yes. I'm a strong yes on this. I think technological innovation moves too quickly for the law to adapt. I think the law is a trailing response to challenges associated with technological innovation, and ethical frameworks help us to manage that. One of the things that I say over and over again to our members, when I speak around the world, is that just because it's legal doesn't mean it's not stupid. And we see too much of that in the marketplace today that there is behavior that feels

creepy; that feels unethical; that doesn't feel right somehow; and yet, it has the cloak of compliance around it. And so, I think, we do need to move to a better understanding of what are the frameworks; how do we apply them; how do we build professionals with the muscle memory and the muscle strength inside organizations to apply those frameworks in a way that's meaningful.

MS. ROBERTS: I think we should call it there to give the second panel enough of their time. So, we're going to hear now about marketing and targeting; and I'll give it over to Stacey Gray. Thank you guys, so much. (Applause)

MS. GRAY: Okay, hi. Thank you. Welcome, everybody. Thank you so much to Cam Kerry for having me here today to moderate this excellent panel. And folks in the back, we've got some empty seats that opened up. Please feel free to come up now or during, and we'll go ahead and get started.

So, first, I want to just very briefly introduce the experts that are here on the stage with me tonight. They're all far more expert than I am in these topics, and I'm very excited about it. You have their bios in the packet, though, so I won't go for too long, but just so you're aware.

From my left we have Danny Sepulveda, who is the VP for Global Government Relations, right, at Media Math, a prominent demand side platform, if that's accurate; advertising technology provider for online advertising primarily. And prior to that, of course, he has two decades in prominent public service, which you can read about.

To Danny's left we have Sheila Colclasure, the SVP, global chief data ethics officer, and public policy. Hopefully, I'm getting that right. Sheila directs the Enterprise Governance Data Protection and Privacy Program for LiveRamp, which we'll also talk about.

To her left we have Tim Sparapani. Tim launched SPQR Strategies. He's the founder of SPQR Strategies. Prior to which he was the first director of public policy at Facebook.

And to his left all the way on the end we have Justin Brookman. Very

excited to have Justin here. Justin has a long history in consumer advocacy and privacy advocacy in civil society. And is currently, how long, Justin, into your new role at Consumer Reports?

MR. BROOKMAN: A year plus.

MS. GRAY: A year plus as the director of consumer privacy and technology policy at Consumer Reports, which has been increasingly active in the privacy and security space here in D.C.

So I'm going to recommend that we not retread some of the grounds that was really excellently covered on the first panel. I think they got into some of the differing approaches of U.S. privacy law and the GDPR, some of the failings of notice and choice, some of the risks posed by the rise of new and emerging technologies. And that, I think, has all been well covered.

But what we've been asked to talk about here today is specifically advertising technology, advertising technology and the closely associated world of data brokers, which I understand even by itself can be a contentious term. And so to start out I just want to acknowledge that these are the two fields that from my perspective at Future Privacy Forum are some of the least understood in the entire consumer privacy debates that we see day to day. Not only are they I think some of the least understood industries, but they are also the industries that tend to be a flashpoint for consumer advocates. There is just a tremendous amount of scrutiny and attention paid specifically to these two industries and we'll talk about why and how much of that is accurate and correct.

Just to level set for the audience on what it is we're actually talking about, I thought I would quote from the FTC's 2014 report on data brokers in which they undertook an analysis of nine data brokers and tried to characterize them and identify some of the risks associated with this field. And I'll add a little bit more to that because I think the field has also changed considerably since even 2014.

There are five characteristics of data brokers when we're talking about what

it is we're actually discussing that the FTC wrote about in 2014. The first is that these are companies that collect data from a variety of sources on consumers -- we're going to be talking mostly about U.S. consumers today -- largely without their knowledge, although that may be changing. And these records may be related to things like voting registration, bankruptcy, purchases often through loyalty programs, online web browsing activity, and many more things that you can get from commercially available or publicly available and often government records.

The second characteristic is that this ecosystem, for lack of a better word, is very complex. Often we're talking about data brokers that are selling and reselling information to each other in ways that may not even touch the end user.

The third is that as an industry we're talking about a vast array of data collection covering nearly every U.S. consumer and I might say nearly every U.S. individual.

And these data sources are combined and analyzed together to often make inferences that are relevant to marketing and advertising.

The fifth characteristic is that these sources can be online and offline. And there is an increasing push towards technology that is able to combine online and offline sources.

That's what the FTC said in 2014. I would add to that that in the last five years we have seen a rise in intermediary platforms that specifically provide a service that I would call crossed by linkage. That is not necessarily augmenting consumer profiles at all, but simply providing the service of demonstrating that the person who owns this phone or tablet is the same person or family that owns this smart television or smart watch or a computer. And this largely just driven by the number of devices that we all have today and the number of different platforms that we're all using to consume content.

Within that field we're going to talk about ad tech facilitators and, of course, just to anchor us in time, of course it's June, it's 2019. The debates on federal legislation have reached their peak. In all the time that we've all been working on consumer privacy we

have seen 16+ either discussion drafts from industry and civil society and introduced bills in Congress just in the last 6 months. So if you need some weekend reading, there's a lot out there in terms of different approaches that you can take to regulating consumer privacy in the United States.

There's also, of course, a tremendous amount of state activity, including specifically we might talk a little bit about the Vermont data broker registry bill, which came into effect this year, and this led to a registration of data brokers operating in Vermont.

So with that level setting, we're going to leave some time at the end for questions. And the structure of this panel is that we're going to talk first about the current landscape. I'd like the panelists to help me describe that landscape, help me describe what the legitimate and good uses are in that landscape, and what the risks are. Where are we?

And then in the second 15 minutes or so we will talk about what the different approaches are that we could take to regulating consumer privacy in the U.S. that would specifically touch advertising and marketing. And then we'll take a bunch of questions.

So let me start first with Tim. Tim, we've talked about this before and I think you do an excellent job of explaining, so I'll start and just ask how is this industry -- advertising, marketing, data brokers included -- different now than it was 10 or 20 years ago? What's changed?

MR. SPARAPANI: Yeah. So thank you, Stacey, for the question and thank you to the Brookings Institution for the opportunity to speak. Let me go back to my roots not at Facebook, but at the ACLU where I led the privacy efforts.

I'm going to make the argument today that this is the quintessential privacy problem of our day. It has been the quintessential privacy problem of the last two decades and it remains completely unaddressed. Despite what you're reading in the papers about four or five goliath companies out of Silicon Valley being the thing that bedevils our privacy, the real issue is that there is an enormous and completely unregulated industry that's been around for 40 years that is buying up data, selling it to whomever they want at all points.

So the reason that Facebook got in some much trouble is because there as a company called Cambridge Analytica that was taking data and reselling it. Okay. There are all sorts of other things that these companies have done which are loathsome, they're obnoxious, they should be regulated, but we should not lose sight of the fact that there is this industry that has been there for at least 40 years, which is buying and selling data. So let me tell you what's happened in at least the last five years.

Five years ago, I went on *60 Minutes* and I railed about this problem. And I talked a lot about the fact that there were companies that were buying and selling data and that you could buy data about anybody, any malady, anything that had happened that was terrible in their life, and it was being sold to anybody who wanted to buy it.

What's happened since that moment is we've moved from a moment where we're talking about list brokerage, companies buying and selling data to and from each other and, frankly, to the governments around the world, and how we've got a moment when we had an evolution in the practices, and now we're talking about scoring of each individual out there. So what has happened is that the companies, many of them in the marketing industry, many of them in the advertising industry, have taken this to the next level. They've taken the data they bought and they have done predictive work on that data, and they have begun to make decisions about what goods and services they are going to offer each and every one of us, primarily online, but certainly when we go into stores, as well.

So first point, we've moved from list brokerage and now we're on to predictive scoring. And those scores are largely almost entirely unrelated. There's no transparency to them. We can talk about that in a little bit.

Second point, this used to be a third party problem. And what I mean by that is companies which you did not interact with were getting data from companies you did interact with and they were selling it to everybody else. This was a third party problem. So it used to be the case that we would probably go ahead and regulate those third parties that were gathering the data. We could go ahead and say, you know, those companies should

stop being able to buy and sell data because we had no interaction with them.

What's happened since then is something really important. Most of the major retailers out there have actually sucked up and acquired at least one of these data broker companies, so they've brought them in-house. So what used to be a third party problem is now a first party problem. And the question about how we define what a data broker is has totally changed again even before we got to the point of regulating it. So we've lost the ability to sort of identify with precision that that's a data broker and that's not. We should regulate that company, we shouldn't regulate that company. Because virtually every retailer is now a data broker, and that's happened just in the last several years and it's happening with increasing frequency.

The third and final point, and I think it's happened just in the last five years and it's a really important transformation of this industry, is that we've moved towards a moment of almost ubiquity of this practice. It used to be that the best companies could buy brokerage lists, right? They could do the scoring and they could be in an advanced position in the marketplace because of their ability to obtain these advanced data services. This stuff is cheap, it is ubiquitous, it is everywhere, and it is again completely unregulated. So we're in a new era and it is affecting every single thing we do online. So let's get after it.

(Laughter)

MS. GRAY: So you gave some really good examples in the *60 Minutes* report of specific brokers' lists that are available for purchase. Do you want to elaborate on a couple of those?

MR. SPARAPANI: Yeah. If you've ever, you know, maybe had a family member who's had an addiction problem, which is about 30 million Americans, there is absolutely a list sale about you and the member of your family who's had that addiction. Every single malady that you've ever had, they're selling that list. Every malady that your family members have had, somebody is selling a list about that. There were rape victim lists; some of those have been removed now, but there were actually people selling victim --

lists of people who were victimized by rape and other sexual assault. And I could go on and on and on.

There either is a list for everything and now there is characterization of people into groupings based on all sorts of appearances and opinions about people's attitudes, so that you're being lumped into groups. So we've taken those maladies, those things that you can't control that maybe your family members have done, maybe they've had a bad moment, they've not been able to pay their bills, and now you're being lumped into those things. And those lists are being sold about you.

MS. GRAY: Thanks. I'd love to get Sheila's reaction. Tim, I think, was correct to point out that this is an industry that's been around 40+ years. Sheila, what's your reaction to this? Can you tell us a little bit about the history there? And do you agree that this field is totally unregulated?

MS. COLCLASURE: Well, by way of background, my prior life was with Acxiom Corp. Some of you may know, certainly we were part of the FTC special order, the resulting 2014 report. So about 18 percent of Acxiom's revenue is actually the collection and cleaning and hygiene and producing a data product. And I can say having worked for that company for a very long time, we didn't have any of those kinds of scurrilous lists. We ran a very careful, thoughtful program. We were a member of the Direct Marketing Association and were primary voices on the privacy promise to the American consumer. We did access to all of the data we used for fraud detection and prevention. And we made that data available for things like banks who are required by law to know their customers. So we built those information tools very thoughtfully with an extraordinary amount of rigor for the products we produced for marketing and advertising purposes.

We innovated a data provenance or a data origins process 15, 16 years ago, where not by contract we actually would go and do due diligence, look at the origin of the data to determine where it came from, how it was collected, what notices were in place, how effective we thought or believed they were, what kind of consumer experience created

the data. We then mapped it forward to use. We have or had, you know, Acxiom did and still does, a data classification program which maps into permissible uses.

So we had a very layered and rigorous approach to ensuring that data was used ethically. And, in fact, the program was called Ethical Data Use. And that company, which is truly -- you know, a portion of their business is data brokering, served large brands and small brands. And I think one of the points I want to make is, in my view, that's very old-fashioned stuff. It has been around for 40 years. And actually data, having a list available like a small hardware store would go in and they would want to be able to find a mailing list -- this is the olden days -- of homeowners in the area, so they could promote they sold roofing supplies in their store. The apartment dwellers probably wouldn't be as interested in re-roofing their apartment building, but homeowners would. So it was a way to create efficiency and control cost and reach out and connect with your audience. That's the olden days.

In the future, of course, data has become infinite. Where we are today, data is a reality. It is way beyond big data. We live in a virtual cycle. The smart devices that we all carry, our little mobile hip computers as I like to all them, consume and create and consume and create. It's the way tech works. We are living what's called the Fourth Industrial Revolution, the Digital Age, also called the Machine Age. And the fuel of the Machine Age is data.

So in my view it's not -- data is, technology is, and will continue to be. The big question is how is it used?

Data is one of the great democratizers. Right? A market entrant who doesn't have the money, the resources, the savvy to compete with one of the monoliths can have some data and effectively compete in the digital space, which is where all of us are living and consuming. Our consumer lives are now very digital. Right?

So I think it's a matter of competition, of fostering innovation, of free speech that data does flow. It is available, but is accountable. And I think that's where the real

debate is. We have acknowledge the reality and the practicality of our economy, of jobs creation, of the need to ensure that America remains competitive into the digital future. So we have to figure out a way to grapple with the reality, but make sure our marketplace is trusted, that we have the right controls in place so that we can foster innovation and competition.

And I think there's a way to do it. I would love a national standard that is accountability-based, has all of these empowerment rights for people. And I think those are a continuum.

One example that bright lines that is for a fraud detection and prevention tool I don't think you should allow "opt out." Having run a program that had those tools available, it was an everyday occurrence that a bad actor would try to opt out. We provided access and they would challenge the data and we'd have to go through this rigorous research to determine if the data was real true from its point of origin. But, you know, these choices are on a continuum.

And I think, what Amie said earlier, I don't if she's still with us, but it's incredibly complex. It's not a one-size-fits-all. Data is really important and its use and its value and its benefits and its potential harm or risk is highly contextualized, and we need a very thoughtful approach to how to get it right.

MS. GRAY: Awesome. Thanks, Sheila. And I definitely what to return to the topic of access rights and opt-outs a little bit later when we talk about how the law addresses this.

And it's true that Acxiom I think is one of the prominent examples among data brokers, both of generally better practices, but also specifically of your access tool. Which out of just curiosity, could I get a show of hands? Has anyone ever used the Acxiom access tool where you put in your information and see what the marketing categories are?

MR. BROOKMAN: It no longer exists.

MS. GRAY: Pretty good.

MR. BROOKMAN: It's offline.

MS. GRAY: Yeah, it's offline and I understand being redeveloped.

MS. COLCLASURE: I'm not with Acxiom anymore, so I don't run the program anymore.

MS. GRAY: Right.

MS. COLCLASURE: But my fabulous colleague, Jordan Abbott, does. And the reason, and I'll just share and I think Jordan would be fine if I shared, they've removed it is the code was old and clunky. And they're innovating a new tool to get ready for CCPA. But Acxiom's way ahead.

Now, I'm with LiveRamp and they are not a data broker. They are one of those linking or data connectivity companies. So we do this -- I think it is a democratizer of the digital marketplace. We enable little companies, new companies, entrepreneurs, startups to enter the digital space and connect with the same power as the big monoliths. So I'm really proud of the capabilities that we've devised while operating a very rigorous, aggressive data governance approach.

MS. GRAY: So, Justin, let me get your reaction to that because I think competition is at the heart of Consumer Reports' mission. I know we've also heard this similar style of rhetoric. Data is democratizing in many contexts related to online advertising for many years. From a consumer advocate point of view, what's your reaction to that?

MR. BROOKMAN: I mean, I've certainly heard this argument over time that privacy law only helps Google and Facebook. Right? It's a very common refrain. I mean, it's not like Google and Facebook were doing badly before GDPR. Like the Google/Facebook rise has been kind of incremental and, you know, it gets passed and it gets implemented. I think it's kind of silly to blame GDPR for doing that.

I think Google and Facebook have viable business models outside of the data broker. So Google can still make a ton of money doing first party contextual ads off of Search. Facebook can still make a ton of money serving first party ads that I think don't

really violate context. To that extent they're maybe better off. But Google and Facebook are the biggest recipients today of third party data. And so I think to argue that it's in their interest is kind of silly.

You know, I think we do have an existing framework for dealing with third party, right, and it's the Fair Credit Reporting Act. And we say, you know, there's no -- you can't opt out of the Fair Credit Reporting Act. You can contest it. You can argue that it's accurate. There are obligations. But we've said for these limited purposes, like credit and employment and eligibility, we're going to allow people to break context. We're going to allow people to share data and there's no rules around it.

For other data, I don't know, I'm not convinced. I think you can make an argument that there isn't the justification for allowing a grocery store to just put in their privacy policy, "We reserve the right to share information with data brokers," then it goes to an Acxiom. Right? I think that that breaks context.

So I want to hear counter arguments to this, but I think there's an argument that data outside of -- we don't need third party data outside of the boundaries of the Fair Credit Reporting Act because I think when consumers do go form site to site or from store to store there's a natural -- I think when we're talking about context, this is the premise of the Obama Privacy Bill of Rights, that it kind of stays in that first party-ish relationship. And rather than force people through consent dialogues on every single site they go to or every store making them fill out a form and what are your 20 privacy choices here, instead the law should accord data practices to that idea of context and to consumers' reasonable expectations.

MS. GRAY: So grounding data in context and reasonable expectations. Danny, do you want to argue against anything that Justin said or what's your reaction to that in terms of --

MR. SEPULVEDA: I think you can add to that. Context and consumer expectations are clearly very important as key principles in the construction of any privacy

law. And I've been through and watched multiple efforts to construct a general law of privacy for consumers.

Justin mentioned the Obama efforts and the Obama administration where Cam Kerry was a key component of that. I was at State when we did that. I was the principal staffer on the Kerry-McCain bill, which I think is still the only bipartisan, comprehensive privacy bill presented in the Senate. And I was on the Commerce Committee working for Barbara Boxer when Hollings moved a comprehensive privacy bill through the Commerce Committee. And I can tell you that in none of those contexts, and I don't believe in the GDPR either, has anyone said that third party data should be illegal, that we should prohibit access to and use of third party data. There are very good uses for third party data in the ecosystem.

The rise in value of first party data has taken prominence, in large part because it is just more likely to be true. It's directly observed. And it's more likely to be useful because you know who you're talking to.

The utility of third party data for marketers and in advertising is really for the expansion of reach. And there you're dealing with probability as opposed to certainty. And the goal with probability, you don't get the same sort of return, but you do have the ability to reach customers that are somewhat like the customers you know or that you believe may be somewhat like the customers you know.

And so the market has kind of worked out the differential pricing in all of that. I do think that the things that were discussed earlier and the things that Cam and his colleague raised in the paper that they produced today around stewardship and the obligations of anyone who accesses data, whether they be a third or a first party, should be consistent and they should be high. And then a consumer should have a much greater degree of capacity to control how the market sees them.

MS. GRAY: When you talk about accessing data can we bring it home to the point of data collection, for example?

MR. SEPULVEDA: Sure.

MS. GRAY: So just to take it back to Justin's point about reasonable expectations and context.

MR. SEPULVEDA: Sure.

MS. GRAY: I think it was the Times that just earlier this week purchased a list from a prominent data brokers and contacted customers on that list. And even if you didn't see it, the basic point is upon contacting people on that list most of them were surprised at the information that was available about them from various government and commercial sources. So it may not be surprising or outside of context or outside of expectations for, say, my grocery store to know what I've been purchasing, but the fact that that same information may be shared, sold, disclosed to third parties that use it to compile profiles while a common feature of the status quo information-sharing ecosystem today, can we make an argument that that's not surprising to most people or out of context or unreasonable? Feel free or Justin.

MR. SEPULVEDA: I'm --

MS. GRAY: Yeah, please.

MR. SEPULVEDA: We're not in that business. We're not a data broker, although we do -- for the purposes for out marketers and our clients, we will access some third party pools of data. We access information from Acxiom, from Oracle, and from some of the others to amplify campaigns.

To your question, it may very well be surprising. I don't know if it's any more surprising than say the fact that TurboTax shares your information with Intuit, which is its holding company, or that the Starwood Hotel Groups has multiple brands and they share -- or that Disney owns Hulu. Most people don't know that Disney owns Hulu. Right?

So then the question becomes what is the utility of that information being available across multiple properties that an individual may not have knowledge of being shared? And how do you balance that against any potential, Question A? And then

Question B, how do you ensure that the individual has access to that information and, depending on which rights you want to assess it, has the right to delete or correct information that might be incorrect?

So I think that the complexity of the ecosystem is such that we do -- while notice and choice will remain a component of any privacy bill, we shouldn't be limited to the notice and choice paradigm, but think about a new paradigm around what are commonly accepted obligations for stewardship, what are commonly accepted and prohibited uses of information, and how do we elevate the capacity of our consumer protection agencies to have both the expertise, resources, and power necessary to enforce those rights.

MS. GRAY: Yeah, and someone feel free to jump in here, too. Do you agree?

MR. BROOKMAN: Yeah, I want to push back on this idea of stewardship or there's accountability or ethics came up as an idea earlier or self-regulation or even this idea of like being a fiduciary. It's like trust us to do the right thing. I think on behalf of consumer advocates everywhere, I think we don't have a lot of confidence in this model.

I mean, corporations exist to make money, and I don't mean that as a bad thing at all. You know, like *Wall Street*, greed is good. That's their role in life. Unless we want to get away from the Milton Friedman concept of they exist for that purpose and that purpose alone, unless you want to adopt some of Elizabeth Warren's governance changes, I don't think we can reasonably expect companies to put societal externalities ahead of their business interests. And if we're not, then I don't think we can reasonably rely upon ethics or accountability to do the heavy lifting to reasonably safeguard consumer expectations.

MR. SEPULVEDA: That wasn't a presentation of what I just said, right? (Laughter)

MR. BROOKMAN: It's a presentation of things I have heard. I mean, you used the word "stewardship," right? And I'm maybe responding a little bit to Trevor's use of ethics in the previous panel and some of Sheila's comments about, you know,

accountability. So, yes, a little bit to you, but kind of more general conversation.

MR. SEPULVEDA: Okay, so then let me clarify.

MR. BROOKMAN: Please.

MR. SEPULVEDA: So what I said is that the end effect of a law should be to ensure that the users -- those of us who are able to access people's information have stewardship responsibilities. And those stewardship responsibilities would not be trust us to do whatever we want with your data or just trust us to self-govern or self-regulate, but rather that there should be a law and that that law should have obligations associated with your access to that information. And that there should be a strong agency with the resources and expertise necessary to enforce that law.

So that's far from saying trust us or self-regulation. I mean, we are well, well past that conversation, and that's fine. I agree. I agree with a -- I've never been an adherent to Milton Friedman. (Laughter) Worked for Barbara Boxer, John Kerry, and Barack Obama. I don't think that we would -- and all of that aside, the point being that we are all agreed, I think that there is a general consensus today, across those of us who have worked in this field for a very long time and represent multiple stakeholder interests, that it is time for a modernization of law, that that law should be strong and that it should apply to all market actors. There's no difference of opinion there.

MR. BROOKMAN: So, I mean, there are a lot of models out there that put a lot of the onus on having a privacy program. Right? There's no actual rules in place, but to behave (inaudible).

MR. SEPULVEDA: Yeah, but who here (inaudible) that?

MR. BROOKMAN: The Washington state privacy bill, the Intel draft privacy bill put a lot of the -- and I'm thinking, from what Trevor is saying, like, you know, we've got this, don't worry about it, putting the process of requiring you to think about privacy ahead of the need for strong, clear limitations on what you can do.

So, you know, within whatever framework, yes, people should be internally

trained, they should be smart, they should do the right thing. There should be consequences for violating the law. But I don't want this concept of having a privacy program to supersede the really more important discussion about clear rules and consequences for violating them.

MR. SEPULVEDA: Sure, I think we can agree on that.

MR. BROOKMAN: All right, awesome.

MS. COLCLASURE: Can I jump in and say I agree? I think the idea about stewardship and accountability is it is a new day. Companies realize that in order to have the right to use data robustly to create benefit and value and be a sustainable ongoing enterprise into the digital future, they have to take responsibility and they have to design with the person in the center. This is this notion of human-centered design ethic or data ethic where it's not just about being a profiteer. It's about data should serve people. I think that we know this.

I also agree that you've got to have a well-staffed, well-resourced, well-trained, strong enforcement construct as a part of any law. But I really worry about this sort of rearview mirror notion of bright-lining this is we're going to stop data flow here and stop data flow there. Because the ability to think with data, to innovate with data, for the flow of digital to actually exist we have to enable that and not artificially try to chop that up because we don't trust business. We have to give a construct that charges business with being good stewards and with being accountable so that the market can operate in a very healthy, trustworthy manner.

And there's always going to be a place for transparency, better, different, newer, modern transparency that's effective for people and those choices and those other controls. And we can decide what all of those are, but I think it comes with this, you know, we're at a new point in time where we've got to have a law that matches the reality of the marketplace and lets the data-driven digital marketplace work, again, in a trustworthy manner.

And I think it gets back to charging those of us that collect and use data with accountability obligations, with program obligations, with stewardship obligations that's inspectable, demonstrable, and enforceable.

MS. GRAY: So to play devil's advocate a little bit on that, it sounds like what you're saying is that we need a federal law that accommodates the current industry as it currently stands. And I think, Justin's nodding his head, that's likely objectionable to a lot of consumer advocates, who are unhappy with the current status quo. Right?

And I want to cite that in my view there's been a tremendous impact of a book published about six months ago by Shoshana Zuboff at Harvard, who wrote a little bit about what you're talking about, about the economic logic that leads to increasing levels of data collection when you combine technology with capitalism.

If you were to create bright line rules they would have to be the point of data collection linked to either consent, which we've seen has all of its faults, right, or some kind of balancing of risks and benefits or some kind of hook to consumer expectations and context. So whichever of those three you choose or maybe some combination of all of them, aren't all of those hooks going to in some way diminish the status quo industry as it exists by eliminating many of the sources of data collection?

MS. COLCLASURE: So I'll be clear, I'm not advocating status quo. I'm not asking for a law that codifies exactly how we're operating today. I'm trying to operate in my enterprise well ahead of the law. You know, the fourth pillar of the company I work for is data stewardship, so we're designing in all sorts of privacy capabilities, control capabilities, transparency capabilities into the way the engineering is designed, functioned, stood up, and deployed because we want to preserve and have an outsized impact on our ecosystem, again, to create this accountability where data's understood, it's under control, it's used for good purpose. There's all the other rights attendant. So we want to have legal certainty and a trustworthy marketplace, so we need a modern law that does it.

And remember, we've talked about this several times, data use is highly

contextual. You have sensitive pieces of data. You have sensitive uses of data. And the big elephant on the table in my view is advanced computing, these new machine learning, deep neural nets, the different kinds of AI agents that are coming online quicker and quicker and quicker.

We've got a great deal of work ahead of us and we need a modern law as soon as we can get one that lets the marketplace thrive, but, again, creates this certainty and accountability with the rights that are variable and contextual across these different uses. An example of that would be the very first privacy law in the United States, the one that's worked very well, it hails from the early '70s, the Fair Credit Reporting Act, which is a data use law and it's accountability-based. And it's what provided our credit economy and fueled the ability for all of us to have access to credit.

So a very important construct, data use in context. When there is a more material use of data with a material outcome I think we need more rigor. But for other uses that are not I would deem material, maybe the control mechanisms and the flow construct is a little bit different.

MS. GRAY: So let's talk about amending FCRA. I think that's a good place to start off with possible legislative solutions here. Tim, I'll turn to you.

Before I do, just to follow on this, in our last panel Amie Stepanovich I thought made a very compelling case that we should not be making distinctions any longer between sensitive and non-sensitive data. But a lot of the examples that you rose have to do with very, very sensitive topics, and it's clear that there should be some limitations on things like that.

Did you agree with Amie? Should there be any distinction between sensitive and non-sensitive?

MR. SPARAPANI: Yeah, the distinction between sensitive and non-sensitive is nonsensical, and Amie's exactly right. Latanya Sweeney proved this out 20 years ago. She's a professor at Harvard. The linkage of data makes any piece of data that

we have about you able to unlock virtually any other piece of data about you. So the idea that one piece of data is somehow, per se, more sensitive, whether it's financial or medical, doesn't really matter, is an anachronistic notion that is 60 years dead and gone. And we should get rid of it because it arose 60 years ago with our initial privacy laws around the world.

And the first iteration of the Fair Information Practice Principles, which was a good idea at the time, but we went on a wrong path. And what has turned out to be the case is that, in fact, because of the ubiquity of data, because of the data broker industry, the idea that a piece of data is somehow more sensitive or less sensitive doesn't make any more sense at all and we should get rid of that notion.

I do think what we're having a problem with here is that we have a series of ethical problems and we don't have laws that are mapped up well to them. And we're talking about ethical issues and we're talking about them in the privacy context.

So we have a series of things that are happening to consumers which are unfair, they are oftentimes unjustified. And we are ending up in a situation where consumers are being forced into a false choice, which is either they get the benefits of technology or they don't. And if they get the benefits of the technology, they also get all the burdens, and that's not how it should be and that's now how it has to be.

So I believe that we are smart enough in this day and age in this country to enact a set of laws and principles that allow us to have all of the benefits, amazing benefits, of technology and of data and of data brokerage. Because there are lots of amazing things that can be done with data brokerage and lots of really important, beneficial uses that responsible companies can bring to the marketplace. And I think that we can make this all come together.

And one of the models that I think is the best model is the Fair Credit Reporting Act. I think it is and remains our best -- it has been and remains our best privacy law. In effect it puts basic limitations on the use of certain data and reporting about

individuals. And it lays out a series of ethical questions which say largely should these things be reported about people? If the data is erroneous about people, should the individual have a right to do something about it? And what happens when erroneous data is used to make an inappropriate decision about somebody or whether it's accurate or not, it ends up with a terrible consequence? What are we going to do to role that back? And that's what the Fair Credit Reporting Act structure does and it has stood the test of time.

And so if it's me and I'm writing the privacy law, I'm not trying to write a big omnibus privacy law because I think that's an enormous lift. What I want to do is take this Fair Credit Reporting Act and expand it out and its concept into -- to take out these issues of data scoring that are inappropriate, to draw boundaries around types of scoring that should never be done, and to find ways to roll back unjustified outcomes for consumers.

I think it's an easy thing to do. I think you can write that bill in two pages. And I think we could pass that act pretty darn quickly and I think it'd be a huge step forward for most consumers. And I think most businesses would benefit from it because I think it had clear bright lines from which to work that wouldn't interrupt with their business models. It would allow them to link data when they need to and continue to provide great services that we all want. So I think that would be a win-win, but I'm an optimist.

MR. BROOKMAN: I mean, I'm a huge fan of the Fair Credit Reporting Act. I'm glad we're all on the same page there. I think it could be tweaked narrowly to kind of more clearly get to some of the more aggressive use cases that people aren't really clear of. There was a really exhaustive complaint filed with the Federal Trade Commission earlier this week by a group whose name is escaping me, but kind of laying out all these consumer scores about how people will use these secret scores to deny people the right to return products and deny service. So I think that probably should fall within the Fair Credit Reporting Act. I'm not entirely sure. It clearly does -- so making that more clear,

I don't know how the Fair Credit Reporting Act would apply to advertising, though. I mean, should it be there should be blanket unlimited collection, retain it for seven

years, no real control around it, no real use limitation around it except for the stated purpose? And you can only contest, well, no, actually I really like raspberries instead of blueberries? I don't think that model works.

I think it actually makes -- I don't know that's what you're saying, but, again, going back, I mean, I think for what Sheila referred to as kind of more immaterial, not as consequential as FCRA, I think we can justify the law enforcing context. Right? Acxiom shouldn't know what I bought at Whole Foods. Google shouldn't know what I do on WebMD. Whatever we've done today to try to get a meeting of the minds on this hasn't worked. And self-regulation, ethics, whatever, all those words, aren't sufficient today.

So I think we do -- again, after 20, however many years, need bright lines to address these issues.

MS. GRAY: Do you want to add anything?

MS. COLCLASURE: I think there's a practicality challenge, especially when you go beyond the material uses that the FCRA contemplates. Of course, FCRA contemplates -- it's a use law and it says any data, any data, used in whole or in part to determine a person's credit capacity, eligibility, or standing is a credit report. So it really binds, if you use data for that determination, then it invokes all the obligations that come with it, and I think that's pretty good.

But in the United States, we've come at other very material uses of data or sensitive and I think there are certainly -- like my detailed health diagnostic data that results from a visit to my doctor is very consequential and very sensitive, at least to me. And so it's protected under a very thoughtful law in HIPAA. And I think we've decided as a culture that we, people, we recognize that there are certain classes of data and uses of data that are more sensitive than others.

I think advertising and marketing has taken a lot of heat, fairly, unfairly. I think there have been a few bad actors that have created some blowback for the rest of us that try very hard every day to get it right and to contribute to a very important financial

engine for the Internet, for free content, free access. I think without the ad-supporting model, I think, the most socioeconomically challenged populations among us would be the ones that were injured the most.

So, you know, I think, again, it's a very complex debate. I think data is inevitable. We are in the digital age. We're going to accelerate. I think there's a bigger conversation to have around advanced analytics, advanced computing algorithms that we also need to pull into this debate because that is a new challenge for all of us and we need to think deeply about that. But we live in a vibrant digital time driven with data. It's an inevitability.

Just quickly by show of hands, how many people have more than one smart device on them today? How many people have a smart TV at home? How many people have a wearable, a watch, a shirt, a bra, some shoes? How many have bought a vehicle in the last let's say 36 months, smart vehicle? What about smart cameras, smart thermostat?

I mean, I've got all that and I want it to all work. I want my tech to work. For that to work, data's got to flow.

Smart medicine, one of mine and I see Stan Crosley here.

MR. BROOKMAN: How many want Acxiom to collect all that data together or tons of other companies? (Laughter)

MS. GRAY: Exactly what Sheila's describing is a lot of the economic logic behind a lot of these companies because the problem is that advertisers can no longer attribute or measure the effectiveness of advertising when it takes place across different platforms. There's no easy way to know that you looked at an advertisement on your phone and then purchased that thing on your device when 10 years ago it might have been very easy to know with relatively minimal tracking. And that's a lot of the push behind this, which I think you're describing.

You wanted to react.

MR. SEPULVEDA: What you were just talking about is the attribution

challenge. And it is, it's a huge challenge. And we actually partnered with LiveRamp on cross-device solutions to many of those things.

But I really don't think we're that far apart as a panel. I don't know if a two-page expansion of the FCRA would solve the problem, but there definitely -- and I think if you're looking to legislation, right now there's a core group of members of the Senate Commerce Committee who have not yet produced a consensus draft, but that will be the primary vehicle, if there is one. And I think it will take ideas and lessons from existing law, including the FCRA, probably some guidance from what the Europeans have done, and some of what the Californians have done, and hopefully add some new ideas of their own. But I believe that that's going to be sort of the moving vehicle.

And as it relates to advertising, you know, we're a programmatic advertiser. What does that mean? That means that we automate the process by which an advertisement goes from an advertiser to be put in front of a consumer. That process doesn't have to be personalized, the idea that you can do that in a contextual framework. We do do it in a personalized framework and we do do it in a contextual framework, and advertisers use a mix of both of those. Personalized tends to be more effective as a matter of return on investment. And we want to be able to continue to ensure that our advertisers are reaching consumers that want to use their products and that those products are relevant to them.

And that kind of frictionless action in the economy is really, really healthy for the economy.

MS. GRAY: So we're going to turn to questions for the last 10, 12 minutes. I'll just react to that, as people think of their questions and raise their hands, with a couple of thoughts on this.

First, Justin, I think you seem to think the panel is much farther apart than Danny does, and that's pretty interesting. And two, with respect to why, Sheila, you mentioned these industries get so much of the bulk of privacy scrutiny.

My reaction to that is that there are two big reasons why this comes up. And one is that I think most people don't see the immediate benefit of this kind of information sharing. Maybe I have slightly more personalized advertisements. Maybe I have free content, which I think we should not underestimate. But it's clear that there are huge values to advertisers. It's clear that there are huge, huge values to advertisers.

And the second is that I think there is right now with the rise of the Internet of Things an increasing concern over the economic drivers. If we translate the online tracking ecosystem and the logic behind it to the offline world, then there is no logical endpoint to the type of data from private life within your home, within your car, that would not be valuable to advertisers or to data brokers. Right? And I think that poses a problem for a lot of people.

Let's take some questions. Cam, obviously the first one's going to go to you.

MR. KERRY: So thank you. Great panel. I want to pick a little bit more at the nub of the issue that Stacey identified. How do you change the status quo? And what's the implications of that?

So, Sheila, you agreed with what Tim said that there were just some atrocious lists out there. So if you think of this big grid behind you as a quadrant, so the upper right is the high social utility and high privacy uses. So let's say the data collection hashtag is maybe "medical research." So there are going to be some things down on the lower left quadrant that may go away, Angry Birds. So, you know, I mean, things that exist mainly to collect and sell data.

MS. GRAY: Flashlight apps that track your geo location.

MR. KERRY: Sure. So talk about where some of those lines are. How does the status quo change? What does that lower left quadrant look like?

MS. GRAY: Tim?

MR. SPARAPANI: Cam, I don't know if this is a direct answer to your

question, but I think one of the things that could be done irrespective of where the utility of data lands on your grid system is that we could import a concept which I think is at the heart of the sentiment behind the Fair Credit Reporting Act, which is that there should be some notion of due process brought into the corporate world on behalf of consumers. Right?

If there is a bargain that is being struck between a business and a consumer and data is the calculus by which much of that decision is being made, oftentimes for the benefit of the consumer, but certainly for the benefit of the business, when there is an error, and there will be errors, what are we going to do to unwind it? And so I want to see businesses take on a process where they voluntarily, or if they don't voluntarily the Congress decides to enact a law that imposes upon them a system where they were is a way to get mistakes undone.

And so I think the question about utility can be resolved either with a high utility or low utility, whether -- because there are going to be errors in both directions. The question is what are we going to do about it?

Shouldn't there be somebody to answer the darn phone or an email or a slack message when something is erroneous that's been done with your data? I would think that that is like part and parcel of the data age because we should get all the benefits and we should be able to undo all the mistakes real fast. That's to my mind is where the world should go.

And it's not a direct answer to your question.

MR. BROOKMAN: Briefly?

MS. GRAY: Yeah.

MR. BROOKMAN: Yeah. I mean, obviously from my comments I'm going to draw the line more to the right, I think, than I think a lot of other people on this panel. I don't want to just get to like the most egregious cases, like the urban strugglers or whatever that shows up on *60 Minutes*. I think like along the quotidian, day-to-day data sharing should be addressed as well.

And this is what the GDPR was designed to get to and, who knows, may one day still get to if regulators in Europe actually want to address that. But I think the way to do it would, again, be to prohibit -- or, you know, if you want to take a -- there are efforts to do a more light touch way, which is, you know, opt out, which is like the CCPA; I mean, opt out to be meaningful and need to be nuclear. They forgot to write that part of CCPA, though they're alleging they kind of did. Do Not Track was obviously designed to address that.

For those of us who really care, there needs to be one easy setting and I think there are thoughtful ways to do that. I think the Wyden bill in the Senate is really thoughtful. I don't agree with all of it, but I think it's one of a more middle ground approach to it to allow all the flowing, you know, for people who don't opt out. But I do think that this is contrary to most people's desires and expectations. And I think that ultimately most people would take advantage of that, so I think you end up in the same place.

MR. SEPULVEDA: I would commend to you a speech that Marc Pritchard, the CMO of Procter & Gamble, gave maybe, I don't know, it was two or three weeks ago on the need for a clean media supply chain.

Advertisers care deeply about the context in which their ads are landing. They care deeply about ensuring that the consumer with whom they want to have a relationship over time feels respected in that process. And they demand from us, from our company and companies like Sheila's, who are part of the middleware between them and the consumer, to provide an addressable and accountable mechanism by which they know that they are reaching the consumer in a way that's respectful and the consumer knows that they're being reached in a way that's respectful.

So to the degree that we move toward and out of the bucket here I think, and that takes out of the ecosystem either dirty supply or dirty tech or dirty -- or bad actors, I think that most of the business community is going to be happy to support that kind of activity.

MS. COLCLASURE: I'll echo that. I'll say having worked in the data

industry for over two decades and, yes, being a part and a strong advocate for co-regulation, industry co-self-regulation, and aggressively enforcing it well ahead of law, because as Trevor said on the prior panel, law sort of drags along, but we always tried to get it right. We wanted to get rid of the dirty. We were serving brands that wanted us to be accountable, wanted to be able to trust that we knew how to get it right. So we worked very hard and we established rules that would keep our ecosystem safe, clear, trusted.

We care deeply. We are trying very, very hard to get it right. Nobody likes the bad actors that have these lists that are insulting, undignified, embarrassed, biased, discriminatory. Nobody likes that, nobody wants it. And so this, you know, pilgrimage through trying to self-regulate, self-regulate, codify, get better and better, stand up rigorous programs, choose trustworthy partners to create a clean supply chain. And now we're at this inflection point where it has come to a head and we need a federal law. We need a federal law that lets the market work, again, in this trustworthy manner and positions the American economy to operate in an interoperable way with the world.

MS. GRAY: We have about four minutes left and I want to get through a number of questions, so I'm going to try this. Let's take three questions and we'll direct them to individual people and hopefully get through a couple in that fashion. So raise your hand if you have a question, we'll try a couple.

If it's only going to be Joe -- all right. All right, Joe, why don't you start us off?

SPEAKER: I'll try not to rant, but this came up in first panel about the notion of enforcement and private rights of action. And a number of people on this panel have already talked about meaningful, strong enforcement. And I just think it's been insightful to ask folks in different industries and different organizations what do each of you think meaningful enforcement looks like? And because this is focused on advertising and data brokerage, do you think that meaningful enforcement exists in this industry?

MS. GRAY: Let's take one more question and then we'll answer them.

Yes, ma'am, right here.

SPEAKER: Just to piggyback off that question, as well. For meaningful enforcement, if it exists in the industry, how can it be improved in the industry in your opinion?

MS. GRAY: And Alan. We'll get the microphone right here. Two questions on enforcement: yes/no to PRAs; and if not, what does enforcement look like? And?

SPEAKER: So my question is a lot simpler. What are the problems we want to solve? And before we engage in a lot of very complex be it two pages or 100 pages of legislation, let's identify the problems. Because oftentimes in panels like these we never talk about that.

And as Sheila just mentioned the embarrassing list, the discriminatory list, obviously that needs to be corrected. Everybody has blessed the Fair Credit Reporting Act. What's the problem there? That incorrect information could deny people jobs, insurance, employment, you know, healthcare, et cetera. So, you know, before you go about imposing a lot of legislation and regulation, identify the problems and solve that.

MS. COLCLASURE: A risk-based approach, Alan.

SPEAKER: Yes.

MS. GRAY: It's a great question, so I think that's for all of our panelists. We'll just start over with Justin. What's the number one problem we're trying to address and how would you enforce?

MR. BROOKMAN: Yeah. So I think people have legitimate interest in not having thousands of random third parties having detailed records about all the things they do. It could be breached. It could be used to give them differential treatment that they don't want. But it's also just a question of autonomy. It's none of your business, right? I mean, going back to the fundamental discussion of the right to seclusion, the right to be left alone, the right to be unobserved I think is a legitimate value people are concerned about, which is why people react so negatively to a lot of this industry's practices.

Quickly, do you want to do enforcement now?

MS. GRAY: Sure.

MR. BROOKMAN: Sure. Yeah, I mean, I think generally there's actually probably more agreement. Yeah, a more robust of FTC with maybe three times the resources, state AGs backing it up, and initial penalty authority.

I do think, you know, echoing -- well, Amie's echoing David Brody, I mean, I think private enforcement is going to mean (inaudible). I mean, you look at with what's happening in Europe, the ICO comes out with a report saying, oh, everyone's violating GDPR, we're not really going to do anything about it. I think just a line of resting and waiting for regulators to do their job -- I mean, look, there are things that if there are ways the private right of action is unfair, then constrain them. But I think people should have a right to act to protect their own interests.

MS. GRAY: So we didn't even get to the ICO report. I should plug if people are interested there is a really excellent, excellent report published by the U.K. Information Commissioner's Office on Friday exploring the legality under the GDPR of real-time bidding, which is a subset of programmatic advertising. Definitely something to check out.

MR. SPARAPANI: I think we're trying to solve two problems, to Alan's question. First we have inaccurate results and we have inaccurate scoring, which will lead to other inaccurate results. And then we have accurate, but unjustified or unfair outcomes and no means of resolving those. And I think we have to resolve both of those things (inaudible) while we try to enact.

And then to the question of enforcement, having advised lots and lots of executives over the last couple of decades, I think the single biggest change that we could enact in order to change behavior would be to hold executives personally accountable. And the way I think that we could do that is something like Sarbanes-Oxley, where we ask for certifications from executives and we require them to actually go through the programs.

I'm actually a huge fan of the intel legislation which forces a program and

requires accountability. And I would like to see executives own what happens in their companies and annually certify to what's happening there and hold them responsible when there's deviation from those certifications materially.

MS. GRAY: And do you agree with Justin's point that the zone of privacy and autonomy itself is the violation, that that's the harm we're trying to address?

MR. SPARAPANI: I'm not sure I understand the question.

MS. GRAY: Clarify?

MR. BROOKMAN: So one thing that the law is designed to address is like people want to be left alone. People want to have people not know about them. Right? I mean, we've passed privacy laws in the past, like the Wiretap Act. Don't listen to my conversations. There's no risk base, so what's the harm. No, some asshole's listening to my conversations. Right? (Applause) People have legitimate interests and caring about that.

MR. SPARAPANI: Oh, okay, yeah. No, absolutely. Yes, this is a real problem. It is a first order problem. I do not know how to resolve it. I'd like the Supreme Court to undo the third party doctrine in *U.S. v. Miller*, and that would take care of it in a heartbeat in my mind. So let's go do that. (Laughter)

MS. GRAY: I can get on board with that.

MR. SPARAPANI: For the next Court session. We can do that next year.

MS. GRAY: The core problems we're trying to solve and how would you address enforcement.

MS. COLCLASURE: Well, I want to echo what Danny said earlier is I don't know that we're that far apart. You know, I'm a person, a human, and a citizen of the United States, and I care deeply about these issues not just for myself, but for my children. And I think it boils down into three buckets and I think data's highly complex, data uses are highly complex and becoming more every day.

Data's infinite and our challenges are this. we need rights of seclusion, so I

want a place in the world where I can be a free and natural unobserved human. I want some autonomy or agency, the ability to participate and be empowered. Right? And then the third bucket or thing that we need to address, and this is where we really need to break some glass and devise modern legislation here in the United States, is this notion of fair processing and what it looks like for the digital age. Because, as I've said, we are -- data is inevitable and digital is a certainty, and it's only getting more complex every day.

From an enforcement standpoint, you know, I think that, too, is complex. Of course we need an authority that's well-trained, well-resourced, well-funded. And I think we need more than just enforcement. I think we need oversight, sort of like the banking agencies. They sit with, they do spot checks, they give an opportunity to cure, and then they enforce. And so I think we need some of that in our enforcement strategy.

For sure we need a federal authority and we likely need the help of the state attorneys general. I think they have a role to play.

Specific to PRA, you know, I think it comes with real challenges, especially for the small business person who it can just literally -- you know, what was that case that was recently in the news about the Disabilities Act and the little coffee shop that literally had been there for whatever it was, 50, 60 years and was a landmark. And an opportunistic trial attorney came after them and literally they couldn't afford it; closed their doors. And that's not that uncommon.

So, you know, private rights of action, I think we have to really understand. Maybe the answer's not nine, maybe the answer is a private right has to be one person at a time and you can't do these big large classes that are just, as we know, having lived through this, big moneymakers for the trial bar and, you know, the person in the class might be 50 cents, literally.

So I think PRA is not a panacea. I think if we want to consider it because we can't staff or train our federal authority or our state AGs well enough, then I think we really have to get down to some granularity and be thoughtful about the unintended

consequence that could devastate especially small and middle-sized firms that don't have resources to withstand one of these settlement negotiations. I think we have to be very careful.

MS. GRAY: All right, thanks. Danny?

MR. SEPULVEDA: So my company's called Media Math because we wanted to apply math and logic and intelligence to what was a previously intuitive process by which an advertiser placed advertisements due to a relationship with a publisher and then hoped that they got a return on that investment. We're really trying to increase the efficiency in the marketplace. And that efficiency enables free services and it enables it marketers and businesses to provide services to people at cheaper rates than they otherwise would be able to.

So the harm that we're trying to prevent as we move forward is to reduce or eliminate any exposure to harm that occurs through that process for individuals. And for those areas where there is a real risk to harm, where you are either using sensitive points of data or inferring sensitive points of data, and it exposes the person as a result to a greater risk of harm, then they should have a higher level of governance. And I think that's where the center of this debate is right now.

MS. GRAY: Okay, great. I think we're just at time, Cam, so we'll stop it there. Thanks so much to the panel. (Applause) I think we have closing remarks?

MR. KERRY: To all of our panelists and to our moderators, thank you all for being here. The event is closed.

* * * * *

CERTIFICATE OF NOTARY PUBLIC

I, Carleton J. Anderson, III do hereby certify that the forgoing electronic file when originally transmitted was reduced to text at my direction; that said transcript is a true record of the proceedings therein referenced; that I am neither counsel for, related to, nor employed by any of the parties to the action in which these proceedings were taken; and, furthermore, that I am neither a relative or employee of any attorney or counsel employed by the parties hereto, nor financially or otherwise interested in the outcome of this action.

Carleton J. Anderson, III

(Signature and Seal on File)

Notary Public in and for the Commonwealth of Virginia

Commission No. 351998

Expires: November 30, 2020