THE BROOKINGS INSTITUTION

FALK AUDITORIUM

HOW WILL A NATIONAL DATA PRIVACY LAW AFFECT CONNECTED DEVICES, APPLICATIONS, AND THE CLOUD?

Washington, D.C.

Monday, September 16, 2019

PARTICIPANTS:

NICOL TURNER LEE, Moderator
Fellow, Center for Technology Innovation
The Brookings Institution

JAMIE BOONE
Vice President, Government Affairs
Consumer Technology Association

MORGAN REED
President, ACT
The App Association

AMIE STEPANOVICH
Executive Director
Silicon Flatirons

* * * * *

P R O C E E D I N G S

MS. LEE: Okay, perfect. Thank you. I am going to get my notes out. Good afternoon everyone.

AUDIENCE: Good afternoon.

MS. LEE: Oh, I need a little bit more than that. You've have about five cups of coffee before you got here. So I'll say it one more time. Good afternoon, everyone!

AUDIENCE: Good afternoon!

MS. LEE: Thank you. I am so happy to actually see everybody here once again at Brookings. I know that we have some of you who are new to a Brookings session. I won't ask you to raise your hand but I would say welcome to you and I know we've got some repeat visitors that come to many Brookings sessions so I would say welcome back. I don't know the last time that you were here and I actually don't know if you were here last week for a privacy conversation but if you were, you're going to get a little bit more privacy today.

I am excited for this particular conversation for a variety of reasons. How many of you have heard that we are trying to pass Federal privacy legislation in the United States?

How many of you heard that about a year ago? How many of you heard it about six months ago? And you're going to hear about it today. And I say that because despite all of the perfect storm that sort of converged when privacy legislation was actually, you know, restarted. We are still at this place where we haven't come up with what we think is really good comprehensive privacy legislation and, in my role, and I am going to introduce the panelists. I am Nicol Turner Lee. I work in the Center for Technology Innovation as a fellow and I basically have three buckets of work that I actually spent a lot of my time on.

The first one is around regulatory legislative policy. I see some friends out here. I have been doing this for quite some time. In fact, I am not going to date myself because I have this young hair style so I am trying to look like my daughter but when we started talking about privacy in the Obama administration, maybe back in 2008/2009, many of us were in that conversation. My colleague, Cam Kerry who is at commerce at the time brought many of us together to talk about online consumer privacy. Back then, when we were just dealing with the internet of things and some of you may remember that.

I also work on issues related to the digital divide and yes, I am going to give a shameless plug. I have a book coming out next year on the U. S. digital divide and I have completed a seven city tour of the United States on how people are accessing digital resources so that will come out soon and then finally I work on issues related to artificial intelligence, particularly algorithmic bias so that ties into the privacy conversation and we'll see how long we have. I've got a feisty group, just wait -- in terms of the discussion. If we get there in terms of other spokes that are under the privacy umbrella, we'll talk about that.

So why did I decide I wanted to have this? Outside of being somebody who focuses on that first bucket, there have been a lot of privacy conversations going on and in those conversations we edge one inch closer, as all of us showed by raising our hand, and one inch backwards. And so, what I am really interested in and I think the panelists up here will help us glean this out and unpack this a little bit, is one, why we haven't made a lot of progress in the last six months and then two, when we look at federal privacy legislation as this umbrella, what are the spokes that are sort of being debated right now?

So all of us have really talked about the principles, Cam Kerry and I sort of have tag teamed on this in terms of the need for some either comprehensive or baseline or whatever you want to call it in terms of the framework but then if you think about an umbrella, there are these little pieces that keep the umbrella solid and under that, maybe some of the issues that we'll talk about today which are cloud computing applications, healthcare applications, et cetera but we've got to unpack while we even -- not even open the umbrella wide enough to figure out how to get the bipartisan support.

So with me today are three folks that I consider to be just wonderful people generally. I have known them for most of my life here in D.C. but also, they've got something to say and I want them to share it from the Brookings stage. So I am going to start at the bottom. She's not an unfamiliar face here at Brookings and she's got a new job! Amie Stepanovich is now the Executive Director at Silicone Flatirons where she is a nationally recognized expert, before then and now, in domestic surveillance, cybersecurity and privacy law. Before that, she was the U. S. public policy manager and global policy counsel at access now and now in Boulder, where she has a much better view than those of us in D.C., you know I had to ask her. Look how relaxed she looks compared to us, right? She's actually moving that forward in terms of privacy and we'll hear more about her in this new role in a few minutes. Let's give her

a round of applause. (Applause)

Morgan is another friend and he's somebody that I used to see often at the oil change place.

MR. REED: Yeah.

MS. LEE: Because we live in the same neighborhood. Is the President of ACT, the App Association where he represents more than 5,000 app makers and connected devices in the mobile economy.

He leads the organization's advocacy and strategy on behalf of small to medium sized businesses on policy issues such as privacy, intellectual property, competition and small business innovation. Let's give him a round of applause. (Applause)

And Jamie. And we've actually had the opportunity to sit in a panel together, another friend. She began her career at CTA as director of government affairs in 2014 and was promoted to seed director in 2017. Her current scope includes policy expertise on self-driving vehicles, transportation innovation and privacy.

And before that, she served in the Washington D.C. office of Representative Beau Schuster a representative from Pennsylvania and the then chairman of the House Transportation Infrastructure Committee. Let's give her a round of applause. (Applause)

David Young, there's a seat for you up here. Call him out since we have no ushers. It's not like church. So let me jump into this first question. We told you we're a feisty group, starting with myself.

MS. BOONE: Will there be a little basket?

MS. LEE: Yeah, right. No collection. We will not have a collection plate at Brookings. So let me start this first question with this panel. Why has this dialogue sort of been extended since -- I think many people in this room probably heard about the need for privacy legislation following the perfect storm of Cambridge Analytica but prior to that there have been discussions but why has it been so long and really for this audience who is probably filing this, how has the debate changed over the last six months? What are the stakes now compared to six months ago. Amie, why don't we start with you?

MS. STEPANOVICH: Sure.

MS. LEE: And let people know again a little bit more about your organization.

MS. STEPANOVICH: Sure. So six months ago, I was actually still in D.C. working on the privacy legislation conversations. That changed about three months ago. I moved to Boulder, Colorado and took over Silicon Flatirons, which is -- I am going to be a little bit bias here, probably one of the preeminent tech think tanks at a law school in the country.

We work on tech policy convenings, student development and entrepreneurship outreach and so I have been leading some of the work that we've been doing outside of Silicon Flatirons but previous to that, I was deeply involved in some of the conversations that are happening in D.C. around privacy and if I were to answer Nicol's question about why this has stalled out, I think one of the reasons is we never got a vehicle. People were waiting for -- there were so many laws. I can count on two hands the number of privacy proposals or bills or principles that I saw but there is this promise of a bipartisan draft law that everybody thought was going to be the one that everybody kind of bought into and tried to make better and was going to move forward and we never got the language on that. And I think one of the reasons for that is people -- the privacy issue continues to evolve.

MS. LEE: Right.

MS. STEPANOVICH: The CCPA is now concrete.

MS. LEE: And for those of you -- that's the California Consumer Privacy Act.

MS. STEPANOVICH: Yeah, the California Consumer Privacy Act is kind of moving into implementation at the beginning of next year. The new stories around privacy keep coming out and people keep realizing that it impacts different communities and different categories of people in different ways and every time that story develops, a new member of Congress decides that they have to be involved in these conversations and be included in the room which means you have to wrap in their staff and get them up to speed and get them to buy into what's being produced and that takes a lot of time.

I will say I don't think it's a bad thing that we're at this point. It means that we are listening to more people, we are taking in more perspectives. It does mean that people may not be happy with the fact that the California law is going to go into effect but again, I personally don't thing that's a bad thing. Having more protections, having companies look into how to apply those protections in the United States so I think the conversation continues to move, people continue to show that they are interested

and involved and we will eventually see a federal privacy law. Is it going to be next year in an election year? Probably not but it's to be continued. It has not stopped.

MS. LEE: Yeah. Morgan, let me run to you and ask you that question.

MR. REED: So, I think one of the fascinating parts, you said six months but I see Aaron Burstein sitting here in the audience and I remember when he was 12 years, 10 years ago working on the Green Paper which was a comprehensive privacy legislation and then you ended up with the FTC for a while, again, pushing comprehensive privacy legislation and there is a well-known think-tank/advocacy group here in D.C. where I think -- they must have had a swear jar in their office that you put money in every time you didn't mention the word comprehensive privacy legislation. I think we all know which group I am talking about, three letters.

So it's not as though this topic hasn't been at the forefront for more than a decade.

MS. LEE: Mm-hmm.

MR. REED: The underlying -- a lot of the underlying problem comes down to what happens in most of these cases that depending on how the language is crafted, there will be winners and losers --

MS. LEE: Mm-hmm.

MR. REED: And so there is a sense that legislation that puts its thumb on one side of the scale or the other is going to meet fierce opposition. Amie was mentioning something that we've all lived through where you get close to a draft and then somebody comes into the room at the last minute and she can tell that story better than I can later but when it comes in the last minute and says oh, I just have three words. And the reality is with comprehensive privacy legislation, I think we all have to be clear-eyed about that reality.

I think the reason you said the six months is I think consumers are becoming a bit more clear eyed about the value of their information and where they sit in the marketplace and I think that with the GDPR, that's the European version of comprehensive privacy legislation, with California, with the attempt in Washington state with facial recognition, I think it's the consumer now that's in a different position.

MS. LEE: Mm-hmm.

MR. REED: And I think before I hand it over, I think one of the last parts is for the first time, we are now seeing market competition around privacy. I don't think anyone can deny that Apple has made a decision to market on privacy. Their CEO has sent letters. They've put that statement out there that we're betting our purchasers of our products want this message so I'd say: 1. Winners and losers are going to make some decisions different. 2. I think the consumers have a better sense of the value of their product and 3. I think you see companies making an active decision to speak to consumers about their privacy and why it has value so I think that's why the conversation is changing and we'll get to a little bit more in CCPA afterwards but that's what I'd go with.

MS. LEE: Jaime, what do you think?

MS. BOONE: Sure, yeah, Morgan and Amie both made really good points that I definitely agree with. You know, last year, we started really having this conversation on why we needed federal privacy legislation between GDPR and CCPA moving. There was a lot of pressure and a lot of pressure not just from consumers but also from industry for that clarity at the federal level.

When it comes to election, you have a flip in the House, you have a lot of new staff. You have -- and in Senate and Commerce, you have a new chairman and a new ranking member, staff that needs to get engaged in the conversation and the policy of a flip and all of the leadership and you have to wait for people to get set up so you know, that takes six months just to get people caught up and making sure that they're having all of the right meetings with the right people and getting that input but I think another thing that has happened is we've seen in the last couple of months there's been this pushback on tech in general and looking at liability with section 230 and now anti-trust and competition. I think privacy is maybe getting a little bit lost in that shuffle where we have all these really big topics and big issues all relating to tech and while I'd argue most -- a lot of them have to do with a lot more than just tech and especially privacy --

MS. LEE: Mm-hmm.

MS. BOONE: It impacts a lot more than just tech companies. I think a lot of those things are getting kind of complacent and it just gets messier. Especially when you have a lot of committees with overlapping or fighting over jurisdiction of who gets to do what and who needs to be in the room when, it gets very messy and I think it makes it harder.

MS. LEE: Yeah, you know, I want to actually stay on that just a second if you don't mind and maybe get some reaction from Morgan and Amie. I mean are we seeing this blurred line or this fuzziness now because it does appear like in the last six months, there has been a lot of press towards you know, big tech shake up and these -- the presidential campaigns have sort of made it their business, interestingly enough to not just necessarily just take privacy but take a whole array of tech issues and sort of put them in the same bucket.

How do we sort of untease out of that or unpack out of those discussions that privacy is still pretty important? You need this probably to start.

MR. REED: So I think one of the problems is and I think it's a bit of laziness. We tend to lump tech into one phrase but the reality is that retail is tech. In fact, we'll talk about it in CCPA a little bit. I mean retail has affinity cards and they have a huge quantity of data and so retail is tech and there's this interesting divide. There's a tendency to lump Facebook, Google, Apple, all of them together but it was interesting on the -- I testified before the House Judiciary Committee Subcommittee on Anti-trust and we were all on the panel. It was Amazon and Apple and Facebook and Google and I was there and Tim Wu and we all went down the line and it was funny, by the end of the hearing, I think it was Congressman Armstrong who was like "Oh, Apple. Yeah, we'll ask you some questions but you haven't really been part of the discussion."

Because they were focused on some of these privacy questions that were coming up and it was interesting how what was happening as they were asking these privacy questions. They were asking questions about well what are you doing with data?

MS. LEE: Right.

MR. REED: And the Apple person was like "Well, we don't really use it. " And another person -- so each person kind of had their own niche so I think one of it is there's a tendency to lump everybody together.

MS. LEE: Yeah.

MR. REED: And I think that's a mistake in terms of how we talk about it and two, I think that to tease it out gets to the key factor, which is look, we are talking about your information and your personal assessment of what its value is, both to you and in the marketplace. What are you willing to

provide to somebody who collects data in exchange for a service?

MS. LEE: That's right.

MR. REED: And I think that's -- that's the tease out. Are you good with that exchange?

MS. LEE: Mm-hmm.

MR. REED: And then I know you deal with this too which is do you think people understand what that exchange is? Do privacy policies even -- we were talking earlier about reading them. I don't know that privacy policies are the methodology to get -- to help people understand that exchange sometimes.

MS. BOONE: I mean I think privacy policies have been written over time in a way that takes the power away from people being able to understand -- I think that we could get there and there's been a lot of particularly academic conversations about what a privacy policy needs to entail and what needs to be shown --

MS. LEE: Right, right.

MS. BOONE: But I don't think that they are written now in a way that allow people to have any idea what information they are turning over, what it can be used for, how long is it going to be held, it's just -- as a sophisticated user of technology, I have no idea half the time.

So people who don't spend their days, their day jobs reading privacy policies, I have no hope for.

MS. LEE: Haha, it's true.

MS. BOONE: And it's not their fault.

MS. LEE: Right, right.

MS. BOONE: It's just that everything is stacked against them. To your point though, I think a lot of these conversations stem from common feelings.

MS. LEE: Yeah.

MS. BOONE: I've been manipulated; I've been abused. I have had my either information or interacted with a company or store or platform that has taken advantage of me and so all of these tech conversations kind of stem out of common feelings and maybe we do need to separate them back out but in a way, and this is going to be a very unpopular point of view. This is like a slay pitch. We maybe need

to bring them together a little bit because there is a little bit of the solution in each of these conversations towards the overall issue of manipulation on the internet.

And once we start pulling that in, like when you talk about the "fake news" or "misinformation" situation --

MS. LEE: Right.

MS. BOONE: That's a societal problem.

MS. LEE: Right.

MS. BOONE: It's not really a tech problem so we have to kind of pull out and think what are the little things that we can do that move us forward across the space. Now those each have their own incredibly nuanced conversations but pulling out might actually help a little bit.

MS. LEE: Yeah, that's why I have been using this analogy of the umbrella with the spokes, right? Because I think part of what's happened in this conversation for me in the last six months is that the spokes are becoming more defined and since there are so many of them, everybody is sort of pitching in what they think the spokes should be on it and it's gone beyond the traditional conversations we've had about consent frameworks and dataminization. It's gone to bias and discrimination and this and that.

But I do have a question because none of you have actually said it in the first ten minutes of this panel, which is the word preemption so I am curious to see if that conversation has gotten better or worse in the last six months before we go into some more details on how we actually get to some type of federal privacy legislation.

MS. STEPANOVICH: I don't know that it's moved a whole lot. I think that everyone's kind of got -- in their corners, what we were talking about earlier, the preemption question.

MS. LEE: Mm-hmm.

MS. STEPANOVICH: I think this just happens. It's not unique to privacy. It happens to a lot -- pretty much everything. Give me an issue and find some way to create preemption to it but we are now looking at California. They've just closed out the legislative session. We'll start to see what the AG does with it and then next year what implementation looks like.

I think that makes this whole conversation harder that we've gotten so far down the road

with California by itself because you've got -- just looking at the politics of it, you've got the speaker of the House, California -- you've got a huge delegation from California, primarily that are democrats and generally will want to support their state and their state's law.

MS. LEE: Mm-hmm.

MS. STEPANOVICH: How do you reconcile that in the House and get it -- something through the house that preempts California but doesn't in a way.

MS. LEE: Right, right.

MS. STEPANOVICH: And then that same thing get through a republican senate. I think the politics on that are really hard so we are just discussing how do you move toward each other in the preemption question and I don't know how you do that without us seeing something to react to on paper. To get people to come to the table?

MS. LEE: I want more reaction to this because we've got 20 plus states there.

MS. BOONE: Sure. So for those of you who don't know and this is D.C. I am not going to forget that I am back in D.C. but preemption is the conversation around the degree a federal law is going to write over state law.

MS. LEE: Mm-hmm.

MS. BOONE: And the reason that it's really unhelpful that people have kind of gone into their corners is because broad preemption, which a lot of people say we just need preemption. We need to preempt all these state laws could impact so much broader than the CCPA. It could go after civil rights law, it could go after abortion law. It could go after anything that kind of comes into the realm of privacy and so you -- even the people who I think really want broad preemption don't necessarily want the broadest of preemption.

MS. LEE: Mm-hmm.

MS. BOONE: On the other side, you could have no preemption at all which could allow people to pass laws that conflict outright at the state and the federal level. So even on this side, nobody goes all the way to the end. I think they at least want basic conflict preemption. They want a federal law that to the extent that it conflicts with state law --

MS. LEE: Right.

MS. BOONE: One standard will take over. And then between those two layers, there are 50,000 other options and nobody has dug in to figure out where they need to be and we were talking -- you've heard many allusions. We've had a really in depth conversation about preemption before we came out here.

MS. LEE: I know. I was like please save some of this for the panel (laughter).

MS. BOONE: But unless we start talking about what real problems preemption is needed to solve and have really honest conversations, that conversation won't go any further. And getting back to my first point, that won't probably happen until we have a vehicle with actual language that allows people to dig into those issues and feel like they are not giving up on their position and until then, it's going to be hardcore digging into the ground and just waiting to see what happens.

MS. LEE: I mean and I just have to -- as you answer, Morgan. We knew about California before California became California. We knew this law was coming and I think I had a coin toss with some friends in the EU who talked about it. They said do you think we are going to have federal privacy legislation before California? I thought I was going to win but I'm not, right? Clearly. So --

MR. REED: Yeah, I always have to remember that nobody does anything until basically, you know, you're waking up and looking at the rope in the morning, right? It's that kind of instinct that lives in D.C. of we'll put it off, put it off, put it off. I think though there are two things. One of the things that came out of GDPR that still to this day is a bit of a problem and CCPA and one of the reasons why preemption is important is even when there are areas that aren't true conflict, you can have overlapping requirements or overlapping buildouts and those favor larger institutions with larger collections of lawyers.

MS. LEE: Mm-hmm.

MR. REED: When you have a conversation, working in the health space which is a lot of what I do on the health privacy space, it's very easy for large institutions to say well first you need to do the DPO and then you need to have all of this documentation on how you are doing privacy by design on your health product and then you need to do a complete six month survey of your data handling on health records and mind you, this is before you've ever stricken a single line of code, before you've written any part of your product, you have to -- your first hire is not a programmer, it's a lawyer. And that works in a large institution where maybe your health product is a skunkworks project and you are borrowing from --

you're going to go to your general counsel and say hey, I need an FTE to work on this but you're in a five man startup who is making a product that say figures out a way to solve diabetic retinopathy. You've probably got five MDPHDs focused on the problem and their first hire is not a doctor so in some cases, the preemption question is not strictly about shoveling off liability risk, which I think some people do. They use preemption to push that off but it's also -- even when the law isn't truly conflicting, where it creates multiple requirements, I often find that my larger company friends are much more comfortable with that than my smaller company members who start to say "Hold on. What all do I have to do?"

MS. LEE: Mm-hmm.

MR. REED: So I think Amie's point about everybody coming to the table and I think there are probably two elements to this. We've talked preemption. The other one is private right of action.

MS. LEE: Yup.

MR. REED: And those two things are the anchor points of this fight where I don't think you're going to have a lot of people coming to the table. We talked about this earlier, all of us, about the fact that we all know in D.C. one of the things that happens is you don't want to give something up that you might want to give up later in the negotiation process.

MS. LEE: Mm-hmm, mm-hmm.

MR. REED: So preemption and private right of action are the ace cards, the -- whatever you call it. The card that you're not --

MS. STEPANOVICH: Trump card.

MR. REED: Trump card. Really?

MS. LEE: (laughter) He said he wasn't going to say it.

MR. REED: Yeah. The trump card in this situation that people are holding on to. So Amie is completely right --

MS. STEPANOVICH: Somebody get that on the record. (laughter).

MR. REED: There are multiple senators in specific and some members of Congress and as you said, I think you hit the nail on the head where you said jurisdictional fights between energy and commerce and judiciary exists but there's also preemption and private right of action which unless we can find a way to come to the table on that, there -- it's going to continue to be a problem and I'll go back to

one of my original points, as much as I love tech and am from tech. I think retail will be driving a whole lot of this.

MS. LEE: Well I definitely here at Brookings have seen more non-tech companies --

MR. REED: Yup.

MS. LEE: Sort of step in the debate because what company is not tech?

MR. REED: Everybody is tech.

MS. LEE: That's part of the issue. I want to, because I always want to be mindful of people in terms of how far they are, deep they are in the debate. Private right of action, explain that to people, Morgan.

MR. REED: Basically, can you hire an attorney to sue on your behalf?

MS. LEE: Yeah.

MR. REED: And to sue a specific company on your behalf.

MS. LEE: Right.

MR. REED: So not the attorney general, not the Federal Trade Commission, not a state agency but you hire an attorney and go sue somebody.

MS. LEE: That's right. And so, Jaime, you know, sort of chiming you in there into this conversation, what should we expect as the new normal when CCPA actually gets passed?

MS. BOONE: Mm-hmm.

MS. LEE: What is going to be our new scenario? Are we going to see more right to legal action by individuals, even if it's a person who wasn't even directly harmed by it? Are we going to see California sort of be the framing quaint for what federal privacy legislation should look like or are we going to just play out California with hopes that at some point something will happen but we don't know what and when.

MS. BOONE: I think it depends on the size of your company.

MR. REED: Right.

MS. BOONE: If you're a big player in California, you're obviously -- you're going to focus there and you're going to try to figure out how you comply with it because I think there are still a lot of unanswered questions there. There are still a lot of things that we left on the table and we've mentioned

retail a few times. The loyalty programs issue has still not been solved, that's been delayed until next year. We still need to see regs from the AG so the next couple of months really and into next year, I think are going to be dominated by reacting to California and how to deal with it. And then you also have GDPR. I mean a lot of these companies that are big in California are also big internationally and are working to comply with GDPR, the ones that are big enough to have it be worth it, I think -- I was reading the other day that there are 1,000 different U. S. sources that have just stopped operating in Europe because it's too uncertain and it costs too much to comply or to try to comply with GD --

MS. LEE: Right.

MS. BOONE: So reacting to those two things and then, you know, if we have a bill to react to, maybe it will bring us back to the federal stage but right now, the feds aren't saying anything so we are getting kind of pushed out of the conversation.

MR. REED: I do want to make one point though that you made. You said big. One of the problems with data is big is not what you think it is.

MS. LEE: Right.

MR. REED: A good example is one of our members did the first sideways keyboard on the iPhone. He has 2. 8 million users. He's one guy in Oregon and he wrote an app. We've got another guy who does Montessori apps for kids, Montessori apps. He's got 1.5 million users on multiple products and so big is not big when it comes to data sets.

MS. LEE: Yeah.

MR. REED: My guys who are in the IOT space, they will have literally billions of data points that they have in their collection and they can be a five man shop so that's why you have to watch out on big because as you know, big is about the data set, not necessarily about the company.

MS. LEE: Yeah. Did you want to say something, Amie or --

MS. STEPANOVICH: Well, it's also about the sensitivity --

MS. LEE: Yes, yes.

MS. STEPANOVICH: To specifically the health sector. I mean I think there are definitely going to be places where people are okay saying maybe I don't want somebody rushing to the market to try to collect 2. 5 billion data sets before they've thought through these issues.

MS. LEE: Mm-hmm.

MS. STEPANOVICH: And I think some of this is a growing pains issue for the smaller companies. We are at -- and had we had privacy legislation in this country on GDPR style legislation 10 years ago, we'd have gone through this already.

MS. LEE: Right, right.

MS. STEPANOVICH: There would have been a pain point, we would have figured it out. Third parties, largely are going to come in and do a lot of this the same way they do with employee records and paychecks and other things and we'd have a system in place. We are using the promise of an inevitable pain point when a law passes to keep a law from getting passed and that means we are never going to get through that which means we are actually creating larger pain points down the road when there are more companies who can do more things who are further entrenched in a system that doesn't have a federal privacy law.

MS. LEE: Mm-hmm.

MS. STEPANOVICH: Where as if we do it now, it's lesser. If we did it 10 years ago, it would have been even easier --

MS. LEE: Right. That's right.

MS. STEPANOVICH: And so we keep pushing it back and making it harder I think on ourselves.

MS. LEE: Yeah, I mean this brings up and I think you saw, for those of you that are here, you saw it sort of embedded into this conversation -- again, the broader dialogue around process implementation. We really haven't gotten into enforcement but I think we've actually talked about enforcement a lot in the general public, right? But I am curious as we look at these verticals of healthcare or cloud based applications and other software, how do we think you know, privacy legislation will actually impact -- I think Morgan, going back to what you talked about -- companies that are small and medium sized, startups, you know, where do we see that conversation happening as we sort of look at, you know, device makers and others who are in this space either directly or indirectly.

MR. REED: So both the app association and CTA have been working on some of these questions in this space. One of the hard parts in working in digital medicine and digital health is

sometimes de-identified information is not good. What I mean by that is to solve the problem. Here's the construct. When you see a physician in your life, if you see your physician at what you consider the top of their game, they will have seen about 29,000 patients, give or take but the number of patients that they would have seen with your comorbidity, your genotype, your genetic makeup, your age, your family history, your everything else. You're lucky if you have a physician that has seen 100 people with your exact makeup and so that puts the physician in the unenviable position of having to make a decision about your treatment based on what they remember from medical school, a couple of classes that they've attended and 100 data points.

MS. LEE: Mm-hmm.

MR. REED: Now there's none of you in this room who do business and make life and death decisions on 100 data points over that kind of stretch so one of the things that digital medicine has the promise to do by using large data sets is to start to say "oh, women of Irish descent tend to react better to this. " Or "if the person has this disease and this comorbidity, we actually find this medication treats them better. " My wife, who is a doctor but of another type; she now works on epidemiology issues, she's always right to point out to me that most of the medical medicine testing has been done on men, even when these women -- even though the medication is assigned to women and my wife is like "Why is this medication being offered up without the (inaudible) research?"

And so large data sets, in some of these cases where we have very personal, very direct information, is the only way we'll discover it and to your point, that's why we would agree when it comes to health information, we need to be thoughtful about how we move forward. The real question is going to be what is considered health information?

MS. LEE: Right, and what is considered personal.

MR. REED: Well, what you eat, where you live, all that stuff starts to be the thing -- it's less about treating the diseases that we know. It's about finding the solutions to the diseases that we don't have an answer for yet.

MS. STEPANOVICH: But medical testing is -- privacy law would not impact who they test the medicines on.

MS. LEE: Right, Morgan, you've been outnumbered this time.

MS. STEPANOVICH: Of that, why are we moving forward with gigantic potential privacy invasions if the actual underlying practices, that have nothing to do with privacy, like who is actually included in these medical tests, we can't solve for it -- let's get that stuff out of the way (inaudible).

MS. LEE: Actually, that's the part that's cool. The FDA and (inaudible) and the FDA and others are working on precertification programs and others so that we can actually do more with large data sets. The FDA -- I am here to actually say great things about a government agency. The FDA is actually putting a lot of effort into exactly that question, which is how do we pull larger data sets in. They've got a whole AI project around this and a lot of it is public pressure and I would encourage people to write -- to encourage them to put pressure on the FDA and members of congress because there is the thought inside of the FDA which is how do we get more information and if you sit down with CMS, the Centers for Medicare and Medicaid and they have CMMI, which does the research in this space, CMMI, we went to meet with them. They say to get a research project out of CMMI will take 10 years.

MS. LEE: Yeah.

MR. REED: Well ten years ago we didn't even have smart phones.

MS. LEE: Right.

MR. REED: So unlocking some of these data sets will actually be key to empowering the FDA and companies to make good applications and to show the effectiveness so it overlaps and I am hopeful we can solve the problem you're outlining by giving them better data because that's part of the problem. Sorry.

MS. LEE: No, I mean I think it's a good point.

MR. REED: I didn't mean to jump on that one. It's my favorite topic.

MS. LEE: I mean I share a similar piece with algorithms where we are actually looking at trading data sets that are, you know, largely male but I don't want to go there, that's another event.

MR. REED: (laughter).

MS. LEE: We had an event like that a couple of months ago. I am not going to go down that aisle yet. But I do want to talk a little bit about, though, go back into these nuanced verticals, right?

MR. REED: Okay.

MS. LEE: Where having access to personal information will matter. I am not sure to the

extent of how much that information has to be personally identifiable but there may be cases, particularly cases of people of color where you want to know what some of those genetic markers are so that you actually have better access to solutions and if they are underrepresented, that's a problem but you know, I am always curious, as we go down this road of privacy legislation, are we going to forget how to nuance that? One from the big company that may be providing that service like an Apple where you can get a lot of health data but then two from smaller companies that are heavily relying on the big companies for data flows.

So I am just curious, you know, I'll go Jaime, to you, I mean CTA, this is part of your business, right? Empowering these new innovations.

MS. BOONE: Absolutely.

MS. LEE: To what extent should we be jumping into that conversation, on how privacy law will affect these third areas or these third ways?

MS. BOONE: I mean I think health and wellness devices is an area where we've had a couple of years not but it's been an area of huge growth and innovation and how you can use these different tools. How you can use virtual reality to help with health monitoring and how you can help with therapy or how you can use different trackers to help look for certain markers that may indicate that your blood pressure is quite higher than it normally is, maybe you should call the doctor, you should go to the doctor and building those in the first place, yeah, it requires data. You have to know what you're building toward and how you define -- because you've mentioned personal information and you've mentioned private information or sensitive information.

MS. LEE: Yeah.

MS. BOONE: Definitions in this debate are so important. I mean half of the amendments that just went through on CCPA were all about the definition of personal information and what are exemptions. What is personal, what isn't, what is sensitive or risky, what isn't? And I think what we are missing a little bit from this conversation is how it's -- how that impacts harm. What is the harm to consumers and how do you draw that line is something always sensitive. Is geolocation data always sensitive? Is -- you know -- x, y, or z, is it always sensitive and do you treat it the same way or does it depend on the application and I think that's a question that still kind of remains to be answered and we

are starting to just see -- we started to dig into the weeds more on that just with California but I think that we'd be remiss to forget that.

MS. LEE: Amie, do you want to jump in on this one?

MS. STEPANOVICH: I think the other side is what is never sensitive --

MS. LEE: Right.

MS. STEPANOVICH: Oftentimes you hear name, phone number, address. There are things that are given as not sensitive information but you start putting those into databases together and then adding other things that you might think are not sensitive and you start painting a really full, sensitive picture of somebody's life based solely on publicly available data and in an era of machine learning, that distinction just becomes almost non-sensical. Eight years ago, there was a machine learning paper that said with two location points, you can identify somebody exactly who they are. Just two random location points. We are getting better and better at figuring out sensitive information from what many might consider non-sensitive and I would say that this distinction is becoming less meaningful.

MS. LEE: Right.

MS. STEPANOVICH: Less meaningful over time because all of that information going into a common center and being analyzed means we probably know more about people than people know about themselves.

MS. LEE: But -- Morgan, before you jump in. so this is interesting. I was at a conference last week, NSF was actually hosting this and it was interesting. We were talking about location data.

A couple of years ago, we would have this conversation of location data. We were all up in arms around that in terms of our privacy. Today, you apply that to certain applications and we are mad if they don't know where we are at because there are several applications that rely upon that location data, whether it's a navigation system, it's a ride-sharing service, it's something, you know. Are we -- and I'll just throw this out as a question. I don't think I've asked this question to any panel. Are we sort of overanalyzing what consumers need and want versus what they are using, you see what I mean? Like in this privacy discussion that's pretty much caught up by us, are we forgetting that some of these things that consumers actually want their data used for?

MS. STEPANOVICH: So this is the Uber question. A few years ago it turned out -- there were three options at that point and time for an app to collect your location data on the iPhone. There was always, never and while using the app.

MR. REED: Right.

MS. STEPANOVICH: And people were selecting "while using the app" and they were getting information after they closed the app so they were able to go a little bit further and people were really not happy with that. Yes, they might want you to have their location information at certain points in time. Few people want every app tracking their location all of the time or beyond where they think they can track you. And so we need to be able to approach it -- and again, back to the nuance of what do people want and are you giving them the option?

I want to be able to enter my address sometimes into a place and not have the app know where I am. Do I have the option to do that? In some cases, that's not true and in some cases it is. Why can't people make that decision for themselves? And if they do want it, then they have the option of turning it on.

MR. REED: I think the problem, and again, Amie is a 100 percent right. There you go, second time. (laughter).

MS. STEPANOVICH: On video (laughter).

MR. REED: On video.

MS. BOONE: Three times and the panel explodes.

MR. REED: I think the problem is that -- and this is something that is very sensitive to my community. It's the whole -- kind of the third party use question of where we go because as you say, you said do consumers really -- do they really want it used and to Amie's point, they want it used in the way that they have the expectation of it. And for those of you who know Lauri Craner, who is at the FTC -- has written a lot about -- do people actually have that fulsome knowledge of not -- not what the immediate use is but what happens next and what happens after that and what happens after that.

And that's where, as Amie pointed out, you get these vertical silos of data built and that creates trouble. The flipside of it is my community depends on third party toolsets to do a lot of things.

MS. LEE: Right.

MR. REED: Third party analytics are a big part of how a smaller company can compete with bigger companies because it ties you into things, it gives you access to a lot of other information and kind of the -- the bogeyman in the room in all of this is interest based advertising because that drives a lot of the conversation that may be separate and apart from what the expectation is. As you said, right? If somebody says I only want it on when I am using the app, but the app monetizes through interest-based advertising, well then, the app company says -- this gets back to who is the customer, right?

If it is monetized through advertising, you are not really the customer.

MS. LEE: Right.

MR. REED: So from the app's perspective, they need that information so their attitude is no, I need that because otherwise I can't provide you the service you want. And to your point is -- this is that questions about where consumers sit, right? How much convenience do they want for a free application that's monetized through use of their data and then do they really know what those things are and that's I think where we as an industry have still not succeeded and that is helping them to understand all of those uses.

MS. LEE: And from a lay person's perspective, or particularly when I've done this book tour, it has to be about privacy, I think it's this concern of consumers that we've become the product, right? And not having any control over what does that actually mean as you talked about before. But I think going back to the first conversation of why we are still here, it's because representatives are trying to take that consumer experience and figure out ways to make that into legislation where they can actually have bipartisan support and everybody has a different angle and where they are coming into the conversation.

MS. BOONE: And if I can just add to that, I think that -- obviously transparency and choice are important and key, and we should be considering that but we need to think about too is the cases when it's not clear whose data it really is.

MS. LEE: Right.

MS. BOONE: Facebook put out an interesting paper last week that was focused on data portability and started to lay out some of the in depth questions of how we deal with data portability and what it is and what it means and one of the most interesting questions was whose data is it. If you -- if I

have my contacts in a service and I want to move that to another service, is it just my data that that is or is it the people that -- their contact information -- do they need -- have they already given approval for me to do whatever I want with the data once I have it there in the first place or not and whose responsibility is that so it's really an interesting edge case that I think we'll start to see more of as we see -- as we get further into the implementation of California that are hard to think right off the bat when you are trying to legislate on it but then come up later as that's a really good point. I actually don't know the answer to that and what does that mean? What are you showing us, Morgan?

MR. REED: When GDPR first came out, one of the questions we asked is if I hand you my business card, does that equal consent? Does she -- in other words --

MS. BOONE: I could give it to Nicol.

MR. REED: Right, exactly. The physical business cards because GDPR doesn't just cover the digital -- the email transaction or anything like that. It's a physical business card and the question that we asked various DPAs and others were if I hand over a business card, does that mean that I am assenting to them taking my information and putting it in my contacts and then if that contact is a service, does that mean that I can go to LinkedIn and pull my data out even if I -- because I don't want you to have it, even though I gave you a business card, which most people would say is consent so it's fascinating to think about, even in physical space how --

MS. BOONE: Absolutely.

MS. STEPANOVICH: Well these are conversations we can have -- we know these are going to be problems. Why are we digging -- that level of nuance. Before I left, we were talking about what types of data should somebody be able to access when they exercise their right to access which is one of the rights under the GDPR. It's something you see in CCPA. Should you be able to access the information you've given? The information that's analyzed and determined about you -- like what levels -- it's going to be the same questions when you ask to erase information that's owned, when you ask to port. Where do those rights apply? These are predictable, knowable questions that are going to have to be solved by legislation and things that we can talk about right now and figure out what the answers are to make sure that they not only work and are workable but work ten years in the future because let's face it, if we do get a federal law, it'll be at least 10 years before we are talking about this again, if ever.

Thanks to California, we are having this conversation to begin with. Let's not forget that when we decide to have really broad preemption, that a state is the reason that this federal conversation started happening.

MS. LEE: I am going to go to questions in a few minutes so if you have a question that is percolating in your mind, just write it down but we'll have some time for question and answer. Before I kind of give you all this chair of giving us a solution, I do want to bring in one other area, which is cybersecurity.

Oftentimes, we are in privacy conversations and just like that spoke analogy, cybersecurity either comes up or doesn't come up or it's the top of the umbrella, right? In terms of the reason we are having these conversations in the first place.

Some legislators are sort of driving their involvement based on the cybersecurity aspect of it versus just general consumer privacy rights. Where do you think we are actually going to fall out with regards to the cyber conversation moving forward?

MS. STEPANOVICH: I think we will likely see security as an aspect of privacy law. It will probably say something along the lines of combination implement reasonable security practices, dear agency, figure out what that means but the FTC's authority in this area has been gutted recently because of a lawsuit challenging one of their actions so we need to have some indication back and I think some of the questions in security and some of the questions in privacy, we are going to start seeing overlap.

We know, and I talk about this on security panels, rarely on privacy panels. We know what to do if our credit card information gets breached. Like how many of you have gotten notice that your credit card information was breached?

MS. LEE: How many multiple times?

MS. STEPANOVICH: You get your identity fraud protection probably from the company that had it stolen. You change your credit card number, it's really inconvenient for about three months because all the auto pays that you had set up have to be reset up again but you know how to figure it out. If your photos on your phone got hacked into, nobody really knows from a personal operational matter what to do. How do you even respond to more personal information getting breached and we're going to have to figure that out from a privacy perspective as well, how do people connect to this non-financial

information, what is the harm that derives from that?

And those are really hard conversations because a lot of that is emotional, mental, long term, unable to come back from it, emotional and mental but it's not the I have five dollars stolen from my bank account or 5,000 or 5,000,000.

MS. LEE: I was going to bring something up, but you might say it.

MR. REED: Maureen O'Halsen has done some work on this and Paula Brewning, who many of you know is also somebody looking at this exact question on -- those of you who are in the legal sphere, you've heard Harms Theory and this question of how does the FTC take action and so it's been very interesting to see. Both of those are former FTC people with inside knowledge of how it works and how do you construct something that creates a harms framework when you don't have direct monetary harm. I think the other part, though, which is important is -- and you touched a bit on this on the control idea is part of giving people back some authority over their data is making sure that it is theirs and that they have some sense of how it's controlled so we are fierce advocates for encryption -- all of that stuff is super critical to providing some sense of self, sense of ownership because it makes a clearer pathway for breaches because if it's encrypted and it's something that I haven't given the holder of that -- the person who is -- to continue holding that container, and I haven't given them permission to access, then if there is a data breach on their end and it's encrypted, then my risk is less.

MS. LEE: Yeah.

MR. REED: So I think there is a tendency for people to -- because back to privacy, the number one thing that people, when we do focus groups on privacy, what they are really afraid about is identity theft.

MS. LEE: Yeah.

MR. REED: It's weird but when you ask people about privacy, what are you concerned about privacy? Well, I'm afraid my data is going to be stolen and then you have to be like -- that's actually identity theft. We are talking about privacy and I don't think the general consumer feels that those are as separated as those of us in the debate do.

MS. STEPANOVICH: Absolutely, I agree with that. 100 percent I think there is a lot of confusion on the part of consumers on what is security or cybersecurity versus what is privacy and they

do get mixed in together. I don't think there will be a large security component to the privacy bill -- more because of the political history of that. We have been trying to get data breach notification uniform national standard with the data security standard for 20 years now but -- going back to that conversation we had on preemption, everyone knows back to their corners and especially when it comes to notification between retail and call providers and banks. Pulling that whole component on top of this already very complex privacy debate has the potential to pull the whole thing down.

MS. LEE: Does that mean that -- and kind of going back to my first question and again, in about 6 minutes I'll go to questions. Does that mean that all of these new areas and I had to go back to the same question I started with, it's just going to make it much more difficult to get the consensus, or, and this is my, you know, rock and roll question here, are there three areas, if you were able to go to legislators and say stop worrying about these ten different things and focus on three.

I'll give an example. So six months ago, no one was talking about online bias and discrimination. Many of you that followed my work know that release (inaudible) important to me. Now, we are actually getting legislators to say it can be involved in privacy legislation but maybe it's not as extensive. We can actually follow up when we get to broader AI implications on that but at least, one of the things that I have been putting out there is update the non-discrimination laws and place those three sentences around that and privacy legislation and move on. Not sure if it's going to happen but it's something that I've publicly said.

Three things that may get us closer to legislation. Amie? I know there are a lot of conversations, this almost sounds like my dining room table.

MS. STEPANOVICH: Actually, I am going to take the opportunity to think a little bit more by making one point because a lot of you guys are privacy people in the room and not security people and encryption was set and just an FYI, encryption is not always the same. There are different forms, strengths, levels so the writing like -- if data is encrypted, none of this has to take place, it's a safe harbor, not all created equal so we'll use that as an education.

So three things. I actually think looking at the -- beyond consent, looking to reasons to process data, the legal basis for processing data is a big thing to get to because it's across areas and it's something to really dig into that can go beyond sectors.

What are the things that we need to provide as legal bases and what is too broad because I think if you talk to the privacy people in Europe, the legitimate basis is like a cop out and was a huge back door to needing a legal basis to get information and if you talk to the other side, they are like this is way too narrow and we need a lot more of a reason and that was another big schism and so digging into that area, I think, is huge.

The lawyer's committee has a civil rights-based privacy law that uses the different privacy rights and then incorporates civil rights protections. I think looking at that at greater depth is going to be super important. To Nicol's point, I think that's something I care about really deeply as well and getting those protections in is going to be important.

And then going -- getting beyond the exceptions piece. So rather than like a thing that we need to concentrate on, it's getting past needing to have an exception for every single industry or non-industry or sector or size of a company and -- as opposed to that, getting to a place where we have a law that doesn't need 50,000 exceptions and is workable and will protect people's privacy into the future when more and more data is going to be collected.

I think that the argument about exceptions in the California law went right up to the 11th hour about how many people wanted things that even know still they are trying to go back and get more written in.

MS. LEE: Right, yeah. Morgan?

MR. REED: I think what Amie said about the exceptions is really interesting and something that we've definitely pushed back on. You'd expect the small business people to say we need a small business exception but that's proven to be very risky and I think you're right so one of the things that was really telling as -- at a Senate hearing about the GDPR, they had Google and Apple and Facebook at the hearing and they asked each of them how much time did you spend to comply and I think Google said hundreds of person years of legal time to comply. And the other companies all followed suit and there was another panel where Garmin, which is actually a pretty small company. They said they spent hundreds of person months on compliance, for a company the size of Garmin.

MS. LEE: Right.

MR. REED: And so I think Amie is right. Making sure that it's not a bill filled with

exceptions because my community actually deals with large data sets where it doesn't matter how many employees they have. I think you have to have a bill that deals with the size and scope and impact of the data set as much as the size of the company. I think that's going to be something that we've got to deal with to right size it.

I think the second part, you said three -- the second part is -- and this is a bit blasphemous and I know I don't have full support for this but I think most everybody here knows that HIPAA is not actually a privacy law. The P in HIPAA stands for "portability" not "privacy."

MS. STEPANOVICH: And there's one P.

MR. REED: And it's one P; just portability.

MS. LEE: Right.

MR. REED: It is about -- and here's a funny little anecdote on this. Unless your doctor actually files electronic insurance claims, technically HIPAA doesn't apply. Like concierge doctors who never file electronic insurance claims, theoretically aren't actually covered. I mean it's an absurdist treatment of it but it tells you something about the fact that the high tech act and the changes to HIPAA are really a tail wagging the dog because HIPAA was about providing portability for patients and getting access to -- and if you meet with ONC, they'll talk about how do we utilize this law to provide better interoperability between EHRs and all that kind of stuff.

So now I look at HIPAA and I want to -- back to this cross-sectoral do we have an umbrella -- I don't know that we want a law that guts HIPAA. I don't think I can ever get that passed but I think Amie is on to something when you say that it needs to kind of not deal with 5,000 -- did you say 50,000 exceptions?

MS. STEPANOVICH: I don't remember.

MR. REED: 99,000 exceptions.

MS. STEPANOVICH: 78.

MR. REED: 78,000 exceptions. I think we have to find a way to be true to what the person is looking for, which is some sense of what is happening with their data, that they have some recourse if the data is misused or used in a way that it didn't intend. That they have some ability to be engaged in how their data is used but ultimately that it still provides companies some perspective and

leeway to -- if I deidentify it, if I aggregate it, that I can still make use of it without that threat being pulled and then my entire algorithm falling apart.

MS. STEPANOVICH: Yeah, yeah.

MR. REED: So I think -- those are two, I think she is right, it has to be sized for all, no tons of exceptions and watch out for financial or healthcare where we may be misusing existing laws in a way that prevents it.

MS. LEE: Yeah, that's interesting, just on that because those have been the used cases that have sort of been triggered, right?

MR. REED: Yup.

MS. LEE: Versus the other ones so that's an interesting way to look it.

MS. BOONE: Are we going to get --

MS. LEE: I was going to say -- this is Congress, okay? What three things can we give Congress --

MS. BOONE: Give us something to react to. A draft would be really helpful. Even if it's a (inaudible) draft. Give us something that we can actually get people to the table because --

MR. REED: Yeah.

MS. BOONE: I think all sides of this debate are interested in having this conversation. We are ready -- we want to move something forward. We see the train coming across the country from different states. What they are going to do on their own if Congress doesn't do something so let's go (laughter). But, barring that, I think it's going to take time and time one because of the nature of the Congressional schedule and then it being an election year and also time to see the implementation of California and react to that and then time to see how other states try and fill the gap and then where we are at.

I am so curious to see where we are going to be in two years. How many others states have something and how much they conflict or if you know -- all built right on top of the California model? Do they take the same -- there are a lot of unknowns out there and I think in two years, we could be in a very different place.

MS. LEE: Yeah, I mean it's like -- it sort of reminds me and now we are going to go to Q

and A but last night I made a really good macaroni and cheese. And when you make macaroni and cheese, you put in the pasta, you put in the egg, you put in the milk, you put in the cheese.

MR. REED: Cheeses.

MS. LEE: Cheeses, right, because you have to have the sharp cheddar baked in and then the shredded on the top, that's how I make it and then end result is its either good or it's bad based on how long you cook it. I had to bring it up because my daughter ate about three helpings of this but when I think about this debate, I think of that macaroni and cheese I made last night because it just seems to me that we all have the right recipe but we don't have the right actors around the table and the right issues and the right temperature and maybe that's the congressional climate to actually get stuff done. And my fear is in the reason that I ask the security question to again tee up your questions, I think consumers are also somewhat getting it conflated, particularly as this election comes through, in terms of what their privacy means, in terms of the public domain of voting and other things and I think we have to get it straight before we get into a place where we get into the next stage of issues which we have not yet determined what they are. So, we are going to take some Q and A. Raise your hand if you have a question. I'd say just identify yourself and keep your question to a question so I can take as many as possible. So we'll start at this side of the room. We've got some generous time for Q and A so if you do have a burning question for the panel, please ask.

MS. RAY: Hi, my name is Debra Ray. I am a graduate student at the University of Maryland and I'd like to know more about what is being said in the conversation about two points. So the first point is not just private right to action but private incentive to act because, you know, just the way the legal framework is set up, it's not enough to just have the right to take somebody to court, you need to be able to go after punitive damages. You need to be able to minimize the risk of walking away with nothing at the end of it so we do need that private incentive to act. Especially -- I mean our Constitution is basically a symbol because it is too difficult to actually enforce our rights and even if we did, it is too difficult to go after damages and hold the government accountable.

So, the other point that I'd like to know more about is infrastructure as a service. My understanding is that companies may begin to start sharing data amongst each other, common data and just the fact that another company owns the data, is information as itself. You were saying before that

two location pieces is enough to identify someone.

Two locations where data exists. That could be enough to come back and gain too much insight into the person. So I just want to know what you have to say about those?

MS. LEE: Who would like to take this question?

MR. REED: One thing, you used the term "too much information." I think I personally prefer the idea of unexpected because what we keep running into is those of us who are privacy nags have a tendency to be like "you shouldn't do this and you don't do this." But then when you watch consumer behavior and consumer expectations, it's actually -- they are like no, I want this or I need this or I don't want a lot of friction in the system. A COPA, the Children's Online Privacy Act has a ton of friction. Parents don't like it; it's hard to get verifiable parental consent so what you are really looking for is instead of too much but is it unexpected? I think there is a point there. On the first point, and I'd like you to take it because this is your space but I think punitive damages for just general non-malfeasance is going to be hard if you don't have intend, I can't imagine that --

MS. STEPANOVICH: No. And I am not a lawyer so I won't jump too far down that rabbit hole but I actually wanted to go to your second point first which is -- I see this assumption of harm in your question and there are a lot of data points -- take ride sharing, for example. We are seeing a lot of request from city and local governments for the data that ride sharing companies have that can be used by the city then to improve services so I want to challenge a little bit that assumption that because there is a lot of data or because there are a certain number of data points, that it's going to be used against someone. I think that it's important to have guard rails on how you use that data and how the city uses that data, how that data is shared but I don't like the assumption that just because there is a lot of it, it's bad, because there are a lot of positive uses there so I think the use and intent there is really important.

Private right of action, that's one of the two -- we started with earlier, those two topics that I think are going to be -- those are the hardest to solve for in this debate in Congress and this is one where everyone is going to be in their corners until we get to that last point where we are down to this last issue of whether or not we are going to get a bill and where do we end up on that and I think it's probably going to go more toward the middle than further to the left.

MS. BOONE: I just want to underscore the importance of your first point, especially for

certain communities. I apologize if what I am about to discuss makes people uncomfortable. I feel like I need to say that. I did a lot of work a few years ago on the security implications of internet connected adult intimate devices and they are collecting -- it's an industry collecting more and more information and it was a weird place where potential victims of these devices getting hacked were getting shamed and victim blamed on two sides. You didn't have enough security and also you use this device to begin with and how dare you.

MS. LEE: Right.

MS. BOONE: For certain communities, the information that is being collected and the potential for them to be pigeonholed or shamed is quite great and that's why a lot of people I think want to have a private right of action built in and to have some of those incentives for them to come forth and file challenges because the potential negative pieces of having themselves in these conversations are quite great for those communities and that's where that importance really comes from and so just to underscore that and to really pull it out what tends to be a fairly privileged conversation in Washington D.C. to say there are other people involved as well who have very very different threat models that they are facing.

MS. LEE: That's right. Thank you, let's go to the second question. Right over here. And then upward this room and I'll come on this side, okay.

MS. DEGRAFF: Great. Jill Degraff from Aperture Law Group. I am curious if in the health data sector, we could actually, you know -- a way I think about it is whether the great privacy complex will actually agree not to have a comprehensive bill in favor of something that's just focused on health data outside of HIPAA and one reason I think about that is that we did have bipartisan support for passage of the 21st Cures Act which in turn was promoting data interoperability. We are no facing a challenge where there has to be data that will be flowing freely portability wise to consumers but into the great unknown of third party apps so there is some urgency and I just wonder whether you think we could peel that off and iterate on it?

MR. REED: Well we know that ONC and I am sure given where you work, you know this. I mean ONC has been kind of raising these questions. There is a -- not a rule -- it's not a notice of proposed rulemaking. I am forgetting the ONC version of this where they've asked on input on that exact

question.

MS. STEPANOVICH: Notice of inquiry?

MR. REED: Yeah, it's a notice of inquiry, thank you. Too many acronyms. So there is a notice of inquiry on that exact question on how do we do portability post 21st century cures and that was -- she's exactly right. That was part of what was kind of trying to be teased out. I think that the problem that we keep finding and I mentioned this earlier is what is health data.

When you start to move into clinical decision support software, that's an FDAish term right around datasets that actually provide decisions for physicians. When you are starting to gather a lot of these data, you may have data in there that might not be traditionally covered and so this question of does data that goes into your EHR -- traditionally we say oh well, if it goes to a covered entity then it's data that's covered by HIPAA but what if I am taking data sets from an EHR that are provided by a covered entity and then I am overlaying it with datasets that I purchased from say Giant and I want location data overlaid on it to see if there is a nutritional deficit there or is there something else in the environment that's causing it.

I think the hard part with a standalone data to try to help interoperability will be -- I don't remember if it was Amie or who said it -- if it was you, talked about the definition's aspects. I think the hard part in that fight is going to be about defining what is health data because there are going to be things that sound like edge cases that aren't so edge cased that are going to make this harder to define but it's a great question and it is something that I know everybody is trying to figure out. How do we get that portability and interoperability in an environment where HIPAA may actually impede?

MS. LEE: And just on that health data questions. It is interesting too because it is health data defined by diagnoses or treatment versus health data like my acts that help me manage my calories that I think are keeping me -- you know, more fluid health data.

MR. REED: Right

MS. LEE: That could actually be implicated, I think, in any privacy legislation that things --

MR. REED: That's right.

MS. STEPANOVICH: And if I can just jump into that as well. So CTA we have a lot of --

health and wellness members, device makers and app makers. We actually recently just put out a health and fitness privacy guidelines for a number of companies that -- our members came together to say -- to explain what the expectations are for that data that's in the inventory. That is not HIPAA data that is --

MS. LEE: Right.

MS. STEPANOVICH: So I think there is obviously action in the industry to address that issue because there are definitely consumer concerns and questions around that but when it comes to actual legislation, I don't think splitting out pieces is where this will go because once you start pulling it off, then you start -- then the next person wants their issue pulled out and then the whole thing falls apart so it's either all or nothing at this point.

MS. LEE: Okay. Next question. Okay, I'll take one question from here and then I'll take one question from here. I am going to move over here so this young man next. So we have another mic right over here. This gentleman, raise your hand just so we can get the mic near you. Okay, perfect.

MS. HASLETT: Hi. Alyssa Haslett with the Cohen Group. I was wondering if you could talk a little bit more about the potential impacts of privacy laws on companies operating in the transportation sector so specifically autonomous vehicles and connected car services.

MS. BOONE: My favorite topic. I do a lot of work on self-driving so -- and this is one area where I have actually been very focused and very interested to see how those -- how the privacy side of the debate and the self-driving side come together and one point that came up when I was raising this with my members working in that space is facial recognition technology.

So there was earlier this year, Senator (inaudible) had a draft facial recognition bill that they were floating around and as I was gathering feedback from my members, I had a couple of different vehicle tech members say this could have a really negative impact on future uses for self-driving vehicles and from two different aspects. One, just from the vision of the vehicle and recognizing people versus animals or a tree trunk or whatever else is out there but two, if you're thinking about self-driving as a -- being the basis for future ridesharing. If you are going and you're getting in your self-driving Uber, there is no one in it to identify that it's you that should be getting in the vehicle. I would imagine and a lot of my (inaudible) thinking about, you know, how do we use -- do we use facial recognition technology to acknowledge that that's the right person that's getting in the right car and going to the right place which is

going to be very important when there is no driver.

So if you are the user and that's your Uber, you're fine, you've already consented. You have the information in the disclosures of how the information is being used. What -- how does it impact someone that it's not their Uber and they go up and just want to take a look in and be like oh what's this and they haven't consented. Can the Uber even scan your face to check if you haven't opted in? What are the consent mechanisms there and what are the disclosure mechanisms there so there is definitely going to be some interesting edge cases like that as well that -- and you could do this for any sector across the economy when you pick something like that and oh, I hadn't thought about that before where there will just be these kind of weird questions.

MS. LEE: And do you want to add on the facial recognition?

MS. STEPANOVICH: I have an interesting story actually. About five years ago, I was at a conference and I can't say -- it was under a certain rule so I can't talk about the identification but somebody from a car company was saying "Well we collect this data and this data and this data" and somebody asked if they could have a private driving mode much like you have a private browser mode where the driver could opt to turn off all of those different types of data collection and the person from the company was clearly appalled and they were like "how could you turn off this data collection?" it is not safe to drive without it and somebody at my table with me, because it's a rule of privacy, people -- looks at me and was like "how did we drive for the last several centuries?" and I think there is a potential for tech to enter in and do things but we need to also think back to the fact that we've done this for a really long time. What data do we need to collect? Like what is the data that is absolutely necessary to collect in order to operate a driverless vehicle versus what is the optional stuff that we are adding on top of that light facial recognition where you could really enter a code to get into the door, much like people did with Zipcars since Zipcar was created.

People may want that extra facial recognition. Like some people may want to look at their phone and have it unlocked but other people might not. Where are the optional data categories?

MS. LEE: Well if I can, I'll just -- because we are doing a lot of work on AI and facial rec. The other thing I would think that is also coming to the privacy legislation and this kind of goes back to my earlier point about how strong is the umbrella to withstand the storms of innovation because if you look at

facial recognition as it is being debated outside of privacy, there is a call to ban it and if that call to ban it happens, then what does that look like when it comes to privacy legislation or are you really talking about maybe data minimization because the faces that are being collected may be faces that are not accurate or technically there are still some problems so the latest case that I heard of facial recognition (inaudible) because I hate the -- little thing about this but I think it's sort of what we have been talking about all day is because the technology is flawed in recognized darker skinned hues, the likelihood of African Americans to be hit by that autonomous vehicle is as likely as hitting a tree trunk because the technology is not refined and so again, this goes back to all of these different areas of technology that are being overlaid and create in the midst of the discussion on legislation and how deep do we go, right? Before we actually come up with something that we can live with that won't implode other parts of the economy or are those conversations happening marginal to this that will find themselves in privacy legislation. You are all following me?

This is like a continuous flow of conversation which is why we are still talking about it. All right, that was my little moderator soapbox. I want to open it up for more questions. Let's go to this gentleman and we'll take one more question on this side and then we'll wrap up.

MR. MURPHY: Hey, Dan Murphy from the Financial Health Network.

MS. LEE: Put it closer. Okay, yeah.

MR. MURPHY: Hey, Dan Murphy from the Financial Health Network.

MS. LEE: Perfect.

MR. MURPHY: So, I was a little surprised to hear you guys say that you don't think that this is going to break down a little bit more along verticals because it seems to me that's where a lot of action actually is happening already. So Morgan, you alluded to the idea that all data sort of can be health data and the financial data ecosystem, all data similarly can be credit data at the same time and we have a lot of laws around that (inaudible) and those conversations are happening in terms of okay, what type of data is credit data and so I am just kind of curious what industries do you guys see as being ahead and why is it that you don't think that that action is going to happen before a national privacy law comes to fruition?

MR. REED: Because you kind of pointed to it. With (inaudible) and a lot of these -- if you

look at how they are structured, a lot of them are harms based. It has to do with the action of -- fair credit -- it has to do with the impact that it has on the person and their ability to get a loan or get a -- almost all of those laws have a harms theory and as we heard from the question over here and from her point about communities that are -- that may have different needs and where the harm might be something that isn't monetary, I think it makes it really hard to do that. Health data is a good example.

One of the areas that has been fascinating to work with on the health community, we had a bunch of roundtables on this. Some patient advocacy groups are okay with privacy but some of the fiercest advocates for not having privacy legislation are people whose children or family members have a disease that doesn't have a cure or a good treatment.

Those people come to the table and they basically say "I don't care about your privacy. My child is dying. I need this -- I need more information." They are zealous advocates for data because they have a family member that's dying and they are insulted when you say how dare you do this so don't forget that there are people for whom they see -- I don't think that it's quite the same but there's a problem with how that will all work because those people will come to the table and say if we have this narrow confine and this narrow construct around health data, what is its impact on orphan diseases or diseases that aren't good treatment mechanisms.

That, by the way, was back to the problem with this. We all talk amongst ourselves but until I sat down with the privacy groups -- I mean, sorry, with patient advocacy groups, that's when I got kind of coldcocked by -- I had been in my own privileged healthy bubble with everything working and I never thought about the implications for people in that case so I think it's hard because you'll be surprised where some of the folks will come from and for your first question, most of the financial privacy space is dominated by harm. Does it hurt someone? And I think that's -- it'll be hard to put that into the same context on health or if we do, it'll be interesting to see how we -- because her point about private right of action, how do we monetize it? How do you make -- seek monetary damages for that. Maybe you'll get it done but that's where I think it will be a little harder.

MS. LEE: Jaime?

MS. BOONE: And I just want to clarify when I said earlier that I don't think health will be split off to be its own separate piece, I was speaking specifically to legislation on the Hill. I think in a lot of

those verticals that you just mentioned and others, there is a lot of work already going on that will continue to go on on the regulatory side or in the industry consensus sides and guidelines and standards. Those things will absolutely happen and continue to happen. I just don't think that Congress will start to split apart privacy into different verticals as oppose to a comprehensive --

MS. STEPANOVICH: I mean ultimately this conversation is happening for a handful of reasons and one of them is the words that Nicol said at the beginning: Cambridge Analytica and if we don't get a solution that solves all the way back for that and we stick in the verticals, I think people are going to see that we haven't done what we set out to do and I think that's one of the reasons that we are going to continue on the comprehensive track. There are so many entities, everything is tech.

Are we solving for the problems when we re-narrow this back down and I think we need to be having this nuanced conversation about things outside of social media because that has dominated the conversation but the solution is -- it's going to have to solve for that.

MS. LEE: Right, it's going to go back to that. Okay, there was another question over here. I see one more question hand. Did I see a hand? Okay, final question and then we will wrap up.

MS. COLLINS: A lot of pressure. I am Kristen Collins. I am a Senior Fellow at the Mercatus Center and this kind of goes to what you were just touching on.

Morgan used the language of markets when you were discussing data and the idea of consumers knowing the value of their data in the market and I wonder what the ethical and political advantages and disadvantages are of using that framework, especially when we think about the collective implications and the ways in which privacy is tied to things like dis-information or security and whether or not framing data in that way will allow us to think more -- in a more integrated manner of these different implications so the idea of -- if we focus on the individual and their consent to their privacy in this exchange, will we be able to get at these bigger questions that are tied into privacy or will it limit our focus?

MS. LEE: Interesting. Why don't we go down the line?

MS. STEPANOVICH: So I spoke about this last time I was on this stage. I actually think this is actually a really bad road to walk down. Once you start getting into how much is your data worth, you start getting into how much can we pay you for your data and that is a super predatory business

model, actually.

Where you start saying “Can we take advantage of certain marginalized communities in order to give them money for them to give up large amounts of their information” and then privacy becomes a privileged commodity reserved for those who can afford it.

So I would prefer we stay away from that framing and start to think of it more as a series of rights the way the GDP and CCPA both framed it.

MS. LEE: (laughter) if you want to say something different, that’s okay. You agreed with Amie the whole time. It’s okay to disagree.

MS. BOONE: Amie has a good point there and I think from the other side of it.

From the innovation side of it, you have the potential then to restrict innovation to only those that can afford to pay for the data and that is not good for anybody. It’s not good for our consumers and it’s not good for all of the potential entrepreneurs and innovators out there so I think I agree with Amie. It’s a really risky path to walk down.

MR. REED: I guess this is the hard part. I mean it’s a good question and I may not have a crisp answer. Here is the thing.

One of the most interesting -- and having worked with Nicol on this, one of the most interesting aspects of smartphones has been the rapid adoption of this technology in communities that are -- have been underserved by tech.

MS. LEE: Right.

MR. REED: Mobile -- smartphone is the fastest adopted technology in the history of mankind by far. Faster than the wheel, faster than fire, faster than the microwave.

MS. BOONE: Faster than fire?

MR. REED: By far. Like by every evidence of how quickly it moved around.

You know, when you talk about marginal communities and impacted -- you have folks in Bangladesh who do not have running water, do not have a street, are on dirt and yet they use a smartphone to check commodities pricing before they go fishing so that they can make sure that they get the highest price by going to the next -- to the right town and while that is -- not in America, you see the same thing going on.

In the Mississippi Delta, the University of Mississippi Medical Center is working to deal with Type II diabetes in a community where they are more than two hours away from a healthcare professional because guess what? That's a community that's poor and doesn't have (inaudible) education but they've all got smartphones and they've all got data plans that allow them to have a lot of data access so I am -- I want to be careful to not be quite as quick as Amie was on making this determination because I think that a lot of those communities actually see value and I'll give you an example. A lot of employers are putting their job applications on mobile devices, especially ones that go to jobs that don't require college and they're doing that because they find that the people who will apply have a smart phone. They don't have a personal computer with a printer but they do have a smartphone and so before we jump to oh, well those people can't possibly make good decisions, I want to be careful with that.

And I understand your point about using the value framework but I don't think that I, as a white guy, should tell people who aren't like me how they should make determinations and I want to be very careful of not being too diminishing.

MS. LEE: I'll help you because I am a black woman.

MR. REED: That's right. That's why --

MS. LEE: And I am going to tell you why. So, Morgan, I think you're outnumbered on this one.

MR. REED: It's fine. As I said, I am just trying to be careful.

MS. LEE: Let me just -- but I'll give you a little bit of credit on something. So I think the question -- and I'll wrap it up with this. I think the question is well-intentioned, right, because I think at the end of the day, the fundamental framework around any of these privacy conversations, around the good stewardship on both the receiver and the recipient in this ecology, right? I want to know that when I give my data, it's done for good purpose, much like when we go to a bank and we give our money to the teller, we want to know that it's going into the vault and not into their pocket, right?

But when you talk about the valuation of data, particularly among disparate groups or different types of people, you do run the risk of exploitation and it already happens. I mean Henrietta Wax, who some of you know about gave up her information for a long time, helped to solve a lot of curable diseases.

It was never paid for and died indigent. And that's partly because we don't have -- and this kind of goes back to what Amie said, the values that operate on the principle that all data is created equal and we don't have a system, which is why we are talking about privacy legislation, that not only is all data created equal but in some respects, all data carries a currency that is valuable to the person and not something that should be used and exploited and manipulated for other purposes and that's where I would leave it, Morgan.

I think that even though people are on smartphones and even though for health reasons they should be paid ten cents for a blood pressure prick in their arm, doesn't mean that we want them walking around with 10,000 pricks in their arms because somebody took advantage of them because they were going to be paid 50 cents.

MR.REED: Right.

Not having food is being hungry and that's another issue that should not be solved by our ability to evaluate people's data. There is no currency in that. So with that, you can see why this is a difficult conversation to have but one that we need to have, right?

I want to thank the panelists. Let's give them a round of applause. (Applause)

I hope that all of you take away from this that this is not the last privacy panel that you're going to go to and I also hope that you take away from this that the issues again of the umbrella that we are dealing with have many spokes and we will soon get there. Let's thank Amie for coming all the way from Boulder to visit us. (Applause)

Thank you again, everyone.

* * * * *

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