THE BROOKINGS INSTITUTION

# WHAT DO THE GDPR AND CCPA MEAN FOR PRIVACY IN AMERICA?

Washington, D.C.

Friday, December 13, 2019

PARTICIPANTS:

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

JEFF BRUEGGEMAN
Vice President, Global Public Policy
AT&T

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

ROSLYN LAYTON
Visiting Scholar
American Enterprise Institute

JOSEPH WENDER
Senior Policy Advisor
Office of Senator Edward J. Markey (D-MA)

* * * * *

P R O C E E D I N G S

DR. TURNER LEE: All righty. Hello, everybody. Good morning. Okay, I go to a black Baptist church and when the pastor says good morning, everybody says good morning. Okay? So we're going to act like we're at my church. Good morning, everybody.

GROUP: Good morning.

DR. TURNER LEE: Okay. I knew you had enough coffee. It's almost 11:00. Okay.

My name is Dr. Nicol Turner Lee. I'm a fellow in the Center for Technology Innovation, and excited to be hosting this panel. It's always difficult as we get to the end of the decade to have a significant conversation, but we thought it was really well worth having this discussion because we're sort of in this sandwich period when it comes to privacy. And let me tell you what the sandwich is.

A little over a year ago, we had something called the General Data Protection Regulation come through the EU that pretty much changed the nature of what privacy looked like. That came at a perfect storm of Cambridge Analytica as well as other privacy infractions that have been mounting in terms of our credit and other institutions. And then leading into January, we'll have the California Consumer Privacy Act, the CCPA, which will be the other part of the sandwich.

And in between that sandwich there's been a lot of discussion and a few bills that are sort of making up a list around privacy. And that would be the Wicker and Cantwell bills if you have not already seen them.

So we thought, and I'm saying the "we" because I'm referring to my dear friend and colleague Cam Kerry, who has been working really hard on this series called The Privacy Debates -- if you have not looked at it, I encourage you to go to the Brookings website and read some recent pieces that he's put together -- we thought this would be a really timely conversation.

Because as these two parts of the bread have basically framed this dialogue on what data collection, use, and sharing looks like, where are we going to take some cues of that leading towards national federal privacy framework or will we diverge, right? Where will there be parts of it that will actually not be relevant to the discussion?

So today's dialogue, I'm joined by some additional friends and I think some really important experts who are taking a look at these issues. I will introduce them in just a moment, but I want to make sure that you all are in the right place and affirm that you are in the right place in this particular dialogue. So we're actually going to start with the discussion and after we start with the discussion, it will actually lend itself to about 10 minutes of Q&A.

A couple other housekeeping notes, please Tweet any activity under what's called the #PrivacyDebate hashtag. And we also have left on your seats an evaluation form. If you find this conversation informative and something useful, I ask that you actually fill that out on your way out, give it to one of our staff who will collect that. So thanks again for being here.

Today I'm joined by experts in this field that will actually delve into this conversation and I'll start again with my colleague Cam Kerry, who is a fellow here at Brookings; Joey Wender, who is in the office of Senator Ed Markey; Rosyln Layton, who comes from next door at the American Enterprise Institute; and Jeff Brueggeman, who is at AT&T. And for disclosure purposes, AT&T is a donor here at Brookings.

With that, let's give them all a round of applause. (Applause)

So I want to jump right into this debate and, Joey, I'm going to start with you, not like you all have anything else to talk about on Capitol Hill. So much has happened in the past 18 months. I mean, this has been a dialogue that's had starts and stops and we now have seen privacy bills come from both sides, which is promising. Due to the bipartisan nature we've had multiple hearings on this, even just as late as last week on it.

So what I'd like to talk to you about is just this conversation around privacy legislation and sort of get this peak from you as somebody who sits on the Hill as to where we were and where we're going generally in the United States before we delve into the influences of I like my metaphor of the sandwich and I'm sticking with it, Joey. I'm just telling you right now. Okay?

MR. BRUEGGEMAN: Okay. Well, I'm hungry, so let's keep that up. (Laughter) So thank you.

I would say we've gone from a world -- so three things have happened. Right? GDPR, the California law, and Cambridge Analytica. I would say those are the three drivers that have changed the course of this conversation over the last couple years. So we've gone from a world of if we were going to pass comprehensive federal privacy legislation to when are we going to pass comprehensive federal privacy legislation? That's the first shift.

The second shift that we've seen in the last couple years because of these three intervening events is what is the scope of what that bill looks like? A few years ago, it would have been a more simple notice-and-choice regime; that people should have notice that their information is being collected or shared or used and they should have the right to say no to collection, sharing, use, sale, et cetera.

That debate has clearly shifted over the last few years. And not only folks on the Hill and advocates, but also industry has recognized that notice and choice is simply not enough for giving consumers rights over their information.

So now we're having a conversation about use limitations, that there are certain things that are not always going to be off the table, whether they be discriminatory uses or what do we do with people's biometric information. What data minimization requirements do we put in place as in you can't, you know, collect that information in the first place? And so it's both this if to when shift and what is the scope of what this likely bill will eventually look like has shifted pretty dramatically the last couple years.

DR. TURNER LEE: So, Cam, I want to jump over to you then because, as Joey's talking about, we're actually seeing I think in some of the new bills, the bill from Senator Cantwell and the bill from Senator Wicker, that are actually starting to look at some of those things. And what I'm particularly interested in since this conversation's about GDPR and CCPA, the extent to which we're actually seeing these new bills, maybe talk about what these new bills are for people who may not know, but if they're in any way influenced by either on either side.

MR. KERRY: Thanks. And I move to strike the last word. (Laughter)

Yeah, they are, as Joey said, they are certainly very much drivers of this legislation, but

they are also benchmarks. So we are dealing with a first set of expectations that has been created by GDPR and more significantly by the CCPA. So as GDPR has been implemented, we've seen many companies that are subject to its very broad territorial reach adapt their privacy programs to the GDPR.

So lots of companies said, you know, in some cases, like Microsoft is one example who said we're going to apply GDPR to all of our services, you know, really as a positioning statement. And then for others it was just a much easier compliance play to say, look, we're just going to have one program around the world.

And so now lots of Americans are subject to GDPR. And then along comes CCPA, which applies to the seventh largest economy in the world and really sets a standard that affects services across the United States. On top of which one-quarter of the congressional delegation, of the Democratic delegation, in the House is from California --

MR. WENDER: Including the Speaker.

MR. KERRY: -- including the Speaker, including a number of other very influential members of Congress, who are saying we are not going to let the federal government role back protections that our citizens have. So any bill is going to have to match up to CCPA.

So that has really set a benchmark and we are seeing the adoption of, and, you know, almost I think as a given in legislation, individual rights of access, of correction, of deletion of data, and portability of data that mirror both GDPR and CCPA. The draft legislation, both the Wicker bills and the Cantwell bills, go I think significantly beyond CCPA in terms of what Joey talked about, limitations on collection, on use, and broader sharing limitations than CCPA. And not exactly like GDPR, but conceptually the same principles, I think looking to having something that is not as proscriptive as GDPR is, not as process-oriented, but, in some respects, also goes beyond GDPR.

I mean, what we're seeing, certainly very explicitly in the Cantwell, Markey, and others' draft is the provisions against the use of personal information in ways that are discriminatory, and that goes beyond GDPR. And not as explicitly, but certainly opening the door to discrimination issues in the Wicker bill, as well. So it's a great start.

DR. TURNER LEE: Yeah. Before we go to Roz on compliance I want to go back to the two of you for just a second. And I want to be mindful of folks who have followed this debate closely and some who are just sort of getting their feet wet in this debate.

When we look at GDPR, and this is an oversimplification that I'm going to make and please correct me if I'm wrong, I like what Cam said, right, this is about a process, a proscription of processes around data use, data collection, data sharing. GDPR -- I mean, CCPA seems to be something that's around enforcement, right, and a much more granular look at what's on and off limits and how do we actually enforce that?

Can you give for the audience maybe a high-level view of what both categories, what each is trying to accomplish before we delve into compliance?

MR. KERRY: Is that back to me? Okay.

DR. TURNER LEE: Yeah, between the two of you. If not, I'll pass it over here.

MR. KERRY: Well, CCPA is, you know, as I see it, is first and foremost about providing more individual control. And so it is those individual rights and it is a right to opt out of the sharing of your data. But in some respects, that is sort of doubling down on the problems that we have today. Joe talked about the failures of notice and choice. And the problem that we have with privacy today is that it really puts all of the burden on us as individuals, as consumers to protect our privacy.

And so what we are seeing is a -- in GDPR, in both the Wicker and Cantwell bills, is a move towards putting more of the obligations on the companies that collect the data to manage that data, to handle that data, or process that data in ways that are consistent with our expectations when we share the data.

DR. TURNER LEE: Right. Joey?

MR. WENDER: The only thing I would -- I mean, I agree with everything you said, but the only thing I would add is that there is more and more of a recognition that there's an asymmetrical relationship in terms of power between consumers and these large companies; that consumers, you can give them all the rights in the world, they don't really understand what these large companies are doing

with their information, how ads and other services are being served to them. And so that's why a lot of this conversation has now shifted to what affirmative obligations are we putting on these companies to help protect consumers?

Because an individual consumer it's just simply not enough to give somebody a 4,000-word privacy policy and say, okay, read this. Okay, cool, you've read it, now you consented to it, it's over. Right? That's clearly just not enough in 2019.

And the only other thing I would add is it's not only this asymmetrical power relationship, it's that these companies themselves have become so much more powerful and so much pervasive in our society and they control so many aspects of our life. So it's not as simple as just, oh, you're handing over your information to a store because you're buying a service. I mean, we're on a whole other level where there is -- and we can talk about opaqueness of algorithms, but there's a whole world in which people are being served news and products and services that you don't understand at all how that happened. And so because of how powerful these entities have become in our society, it's incumbent on us to put more obligations on them in order to level the playing field between the consumer and the company.

DR. TURNER LEE: Yeah.

MR. KERRY: Yeah, some of these companies. I mean, there are --

MR. WENDER: I would say, you know, listen --

MR. BRUEGGEMAN: Yeah, of course. Of course.

MR. WENDER: I will say this, the last thing I will say is that's what makes this conversation so difficult is that Google -- let's just say the words, Google and Facebook become the examples, right, that everybody uses for the Internet or for these companies. But the truth is Google is not like Facebook. Facebook is not like Google. And Google and Facebook aren't like the millions of other online companies.

So the rules we put in place can't just be for Google and Facebook. We have to do it in a way that recognizes there's a huge diversity of services and websites out there. And, frankly, that's what makes a lot of this so challenging.

DR. TURNER LEE: Well, that's a nice shift, Roslyn, to you, right? Because if the -- and thank you both for sort of answering that question because I think it's inherent to this conversation. If there's a shift towards companies, then there'll be a shift towards compliance. Right?

And I was picking up -- my great research assistant, Kaitlyn Chin, helped find a data stat that I want to share with the group from the International Association of Privacy Professionals and Ernst & Young who estimated that Fortune 500 companies spend $8 billion on GDPR compliance and it's anticipated with CCPA compliance that they're looking at about 55 billion. So those are huge compliance costs, particularly, you know, if we're shifting that burden to companies.

So, Roslyn, what I'd like to find out from you, are these real and actualized costs? Are they areas that we should be paying attention to as we shift the regulatory burden? And what impact does that have then on us really creating a benchmark for privacy?

MS. LAYTON: So, Nicol, first I want to start by saying thank you for this invitation and also to Cam and great to meet my new friend here, Joe and Jeff. And just to say, you know, I'm next door at AEI and we've worked together, Brookings and AEI for so many years, we like you so much we moved our office to be next to you. (Laughter)

DR. TURNER LEE: I know, that was kind of like huh?

MS. LAYTON: But I'm going to make some remarks today which is going to reflect my views. AEI doesn't have a view on privacy itself.

And to keep with our idea about the sandwich, as a researcher what I'm looking at is what's in the sandwich? Is it made with Wonder Bread? Is it whole grain bread? You've got avocado in there? Is it a vegetarian? So I'm actually interested in what is the sandwich.

And when I look at -- and also, I live most of the year in Copenhagen. I work at the university in Denmark, at Aalborg University, and my research is published there where I'm looking at the outcome of the GDPR 18 months after it's been in place, and I'm comparing now what we have as CCPA. And so when I look at the differences of these two laws, for me it's about the numbers.

I mean, GDPR has 45 specific regulations around what the company has to do. CCPA

has 77, so it's even more stringent. And the challenge for me is there's a law put together in less than a month, no testing around the provisions that were adopted. The folks who did this they just made it up and said let's put an 800 number on the website. I mean, they just pulled these things together, there's no testing associated with it.

But the early kind of data that we have in terms of companies having to get ready for this is that it's between $1 million and a hundred -- minimum and $100,000 to comply and 1 million. And, you know, maybe in Europe it's been 9- to $10 billion for GDPR. The CCPA is even more than that. We're talking on order of 55 billion, 70 billion. That's 2 percent of the GDP of California.

And the California Department of Justice itself has published a cost-benefit analysis which is giving 14-to-1 costs over benefits, meaning that the cost to set this up -- 55 billion initially, another 16 over 10 to 15 years -- compared to only $5 billion of documented benefit. So that's not a great return on investment.

The other challenge there is that the 99 percent of the companies in California have less than 500 employees. So $100,000 is more than the entire cost that a typical company spends on their entire IT system. So this is going to be extremely challenging for small- and medium-sized companies.

And the other part that we've seen already with GDPR, which I think policymakers need to wake up quickly, is that it has been the reward for the largest companies. We've seen in 18 months that Google, Facebook, Amazon, they have increased their market share in the European Union. They have increased their revenue. In fact, users continue to go to those platforms to the detriment of their competitors who have lost market share. They have lost the ability to track venture capital. And we don't see small- and medium-sized companies growing.

So if you look at the United States, we had 40,000 startups last year, still a wonderful place to innovate. Things are going great. I'm really concerned about we're going to kill the golden goose that laid this golden egg.

And I could give you my wish here, I would go back in time to 2012, when Cam was at Department of Commerce and he was so brilliant.

DR. TURNER LEE: I don't know if he wants to go back to the department.

MS. LAYTON: He had this brilliant idea for a consumer --

MR. KERRY: Depends on which administration. (Laughter)

MS. LAYTON: But he -- actually it's interesting, there's a moral to the story. They had a very -- a wonderful multistakeholder-based standards, technical-based solution, a Consumer Privacy Bill of Rights, which was not all controversial. We weren't able to do it. But the Europeans saw that it didn't happen, they came in with the GDPR and we missed this opportunity. So I hope we don't miss it again, but, you know, the brains are here, you know, at the end of this panel in terms of getting the right solutions.

DR. TURNER LEE: But I want to just, before I leave from you on the compliance, what are these costs?

MS. LAYTON: Yeah.

DR. TURNER LEE: Are they the cost of manpower? Are they the cost of sort of recalibrating systems? You know, we hear "costs." What are they?

MS. LAYTON: The number one cost is a privacy consultant. It is a wealth transfer from the companies themselves to the privacy lawyers or consultants. IAPP have doubled their membership globally.

So the second highest costs are the IT costs, but essentially you could say, well, look, those companies, could you spend a million dollars innovating your products and services? Could you do different things with that money? No, we're paying the privacy lawyers and the privacy bar. They're getting rich off of this.

DR. TURNER LEE: So, Jeff, I want to go to you. I mean, we have you up here, you know, as I mentioned in the disclosure that AT&T does fund Brookings as well as a whole lot of other companies. But I was really curious to get a company on the panel that would actually speak to how this is actually going to affect them.

So Governor Brown, you know, signed the California Consumer Privacy Act in July 2018.

The press basically touted that industry was okay with it to a certain extent, right, in terms of those provisions. And it gave some industry momentum to sort of look at how they could either comply or get this done.

So I'm just really curious, do the CCPA change the way that AT&T or other companies will do business? Are you worried by these compliance costs? Or kind of going back to Joey's original comment, you know, do you see this as a way to sort of have that pressure placed on you to just do better? You know, I'm really curious how you all are looking at this.

MR. BRUEGGEMAN: Well, first, I would echo thanks for hosting this event and all the work that you and Cam are doing on privacy because I really do think we're at a moment in time where there's an opportunity here.

You know, AT&T has long supported federal privacy legislation, back to the excellent work that Cam did in the Obama administration. But California really crystalized this as an issue that's going to hit every type of company, right, from the dry cleaner to other retailers to any company that uses data. So I think it did broaden their perspective and broaden the industry engagement on privacy.

At the same time, just to unpack what California really -- the process, it started as a ballot initiative in 2016. Then the law was adopted that summer. It is taking effect next year.

DR. TURNER LEE: Right.

MR. BRUEGGEMAN: And then the state AG is now drafting regulations that will take effect sometime next year. So we're still filling in what the law is going to mean. And then the ballot proponent is back with another initiative on privacy that he is putting -- going to try and put on the ballot next election that would take effect in 2023.

So I think, on the one hand, it has helped a lot of companies get over that, okay, I'm investing, as Roslyn laid out the numbers, we're investing in the systems to give consumers the tools to manage the data to comply, so it's a lot easier to say let's have privacy legislation. On the other hand, there is a lot of concern about what about the next set of regulations in California or what about another state doing something different? And given the amount and the cost of doing this, it is extremely

concerning to business to then say I may have to do it, you know, 10 different ways going forward.

So on the one hand, it's catalyzed interest in privacy. On the other hand, it's made it easier, I think, for industry to get behind strong privacy regulation because you were already -- you know, a third of the economy is now doing this for California.

DR. TURNER LEE: Yeah, I mean, it's all of it. I mean, when GDPR went into effect and we started getting those pop-ups, it seems like commonplace now, you know, you get them, most people just sort of accept them and they keep moving on, but it seems like, again, I think on the compliance side you actually have to be able to comply and be able to institute those systems.

But I want to talk about consumers, though. Right? Because at the heart of this, even though there may be more burden on industry, even though companies are sort of either going to be forced into sort of this state or not, do consumers actually benefit from any of this stuff going forward? And I'll start with Roslyn. Let's put them back in the conversation.

MS. LAYTON: I think the best statistic on this, 18 months after GDPR, the consumer trust online for Europeans is at the lowest point it's ever been in the 20 years that they have kept the statistics, Euro Stat. You can look for yourself. That's stunning to me because this is reflecting a long period of time the Europeans have tried to do more and more regulation, but the challenge is because of the approach they've taken, only half of the companies comply. So it's really a sense of set it, forget it. You get the pop-up in your face, but the people don't accept -- there's not a culture of compliance.

So you may put all the regulations in the world, but if it's so expensive that the companies just say we're not complying, remember the data protection authority's in EU, they don't have more funding, they don't have training, so they can't enforce all of this. They have to pick and choose what they're going to enforce. So the consumers are really resigned.

And the other part about it is the small- and medium-sized companies don't grow. And that was the -- the real challenge is that there's not a more robust ecosystem as a result of this. And something we need to think, what are we going to get if we go to California?

DR. TURNER LEE: And couldn't the argument be, I want to jump in this, but couldn't an

argument also be made, Roslyn, that sometimes the consumers donate need access to content because the companies can't comply. So remember right after GDPR a lot of U.S. newspapers just fell off the grid --

MS. LAYTON: Over a thousand --

DR. TURNER LEE: -- because of that.

MS. LAYTON: Those were a thousand U.S. firms, no longer work in the EU. Williams Sonoma, you can't even look at their recipes.

But there is a missing component in this policy is that we don't have a consumer education component, which we could have a tremendous difference if we had, you know, digital competence training or we had -- we incentivize the companies to offer training for their users, for example. Because then people would feel empowered.

DR. TURNER LEE: Cam, do you want to respond to this?

MR. KERRY: Yeah. I think we need to put GDPR a little bit in perspective. I mean, I agree with some of what you said, Roz, about the effects. But I think there are some things, you know, the extent of innovation, the venture market, the impact on SMEs in Europe, I'm not sure you can necessarily lay that to GDPR. I think some of that is endemic to Europe and the European economy has not been that strong.

But I think the effects on the advertising market has been clear. I mean, it's clear that both Google and Facebook have gained share. That data, I think, is pretty robust. And I think that does raise competitive issues for how we deal with the sharing of information and the impact of legislation on the advertising markets. We don't think we can fix competition issues with privacy legislation in the States, but we do need to understand intended or unintended consequences on competition from doing that. So that's going to be a critical discussion going forward.

I think GDPR has had -- one beneficial impact has been to force people to look at their data governance. A lot of process involved, but the process of saying what data are we collecting? Why ware we collecting it? What are we doing with it? It's an important step in the process. It's maybe a little

too -- you know, because of the regulatory requirements it's kind of too focused on making lots of records of what you're doing. We need a more flexible approach.

But those pop-ups, GDPR is not all about consent. In fact, it sort of moves things away from consent. But it certainly doubles down on consent where it's used.

DR. TURNER LEE: Joey or Jeff? Both of you come in.

MR. WENDER: Yeah, a lot of people lamented when California -- excuse me, Europe went first. That somehow that the Europeans were now leading the world on privacy. And a lot of Americans here said, oh, my god, how did we let this happen?

Now, but there's a huge benefit to that, though. And the benefit is they've gone first, now we can learn from their mistakes. And beyond Europe, the states are the guinea pigs. Right? They're the ones that are -- California has gone and other states are going to go, as well. So what Congress is doing right now is not only looking at what's happened in Europe and what's happened in California, but they're also looking at all the other states and state legislatures that are now proposing legislation.

So the hope is, and I make no guarantees about the ability or wisdom of 535 members of Congress to pass a perfect bill, but the hope is -- the hope is -- that somehow we will learn from all of these intended or unintended consequences of Europe and the state bills to pass something great.

DR. TURNER LEE: Jeff, you want to jump in?

MR. BRUEGGEMAN: Yeah. I would second that. I think there's a real opportunity to let's learn from both California and the GDPR. Let's take the best of what is in there. As I said, companies have already invested heavily to comply, so there's a strong foundation, but then let's avoid some of the mistakes.

And I would go back to a point that Joey made earlier. I think if we're successful here, things should get easier for consumers, not more frustrating or more complicated. And I think that should be one of the lessons from GDPR that, you know, to the extent that we can identify either types of data or uses of data that really concern consumers and put strong restrictions on those, then let's not put everything into that basket and complicate their lives for just routine transactions on the Internet.

And let's also make sure we're avoiding the unintended consequences about, for example, if you restrict sharing, but not using data, do you end up helping certain companies and not other companies? And I think the frameworks that we've seen introduced, you know, there's a lot of similarity and a lot of overlaps in the thinking that I think shows there's a lot of consensus building on some of these issues that -- you know, but we should always think about the consumer as the one we're trying to serve.

And I guess one last point is I think sometimes, particularly in Europe, it's viewed as privacy is a trade-off for other things. And, you know, consumers benefit from whether it's a free ad-supported website or a new use of data that helps make a product better, so we need to give them both. Right? We need to give them strong privacy and security protections and all of the great things that can happen from using their data. And we really shouldn't view it as a trade-off if we do this right.

DR. TURNER LEE: Okay, good.

MS. LAYTON: I want to make one last point there. I think part of this process of learning from the different approaches is I actually think we'll come again to appreciate the American privacy tradition. It's over 200 years old and it is quite robust in terms of protecting individual privacy, particularly against the administrative state.

And it has also had a tremendous reliance on the importance of recognizing the public's right to know. So you have some terrible situations in the EU where murderers or child predators, they're able to erase the records about their crimes, so that you can't -- you know, there's invaluable public information that cannot be accessed anymore because of this fundamentalist approach to data and sort of individual command and control rights.

But just the one thing I would say about the U.S. approach, people forget that we have over two dozen privacy laws in very specific cases because we follow an extreme democratic approach where we would identify the harm, Congress came forward, actually has done tremendous amount, where there are industries where they would identify this is the problem, this is the harm, this is what we're going to do about it. So there are privacy regulators all over the U.S. and we have to be careful that

we don't torpedo the existing rules that have been developed over, you know, decades and centuries in the U.S., but also to appreciate what's there and how do we complement that. We don't want to dismantle it, but learn from those things.

And the consumers and voters have spoken because they appreciated the American approach, said we're going to identify the dangerous uses of data. We're going to deal with that, but we're going to not assume that every use of data is wrong. We're going to allow permissionless innovation. And consumers have value that, you know, the United States is today one-third of the world's Internet economy.

DR. TURNER LEE: It's so interesting. I'm sitting here writing like a whole lot of notes. Some of the questions that I sent you previously and some I'm going to actually give you now. Right? Because I think this also brings up -- and I think the point around GDPR being placed within an American context is different, right? We have a different relationship to the Internet. Clinton-Gore, we made it free. There was a reciprocal relationship.

That's a little different from what we actually see in Europe. And, you know, Cam and I have been in conversations where Europe is really clear, you know, without really strong privacy policies, innovation may be sacrificed, but that's okay, right, as long as people are protected.

But I do have this question because, again, for the purpose of why people are here, we're no longer talking about GDPR. We're talking about a state law in the United States that in many respects recognizes the cultural context in which we all are consumers.

So I'm really curious now that we have California coming into fruition and we still have federal privacy legislation unsettled, which side will we err upon? Will we try to take those lessons from GDPR, fill in the blind spots around compliance, and go along with California for about three to four months before federal legislators do something? Or will we look at the federal legislation a lot more carefully based on the blind spots that are in the California law? Just curious how California changed the nature of the game for federal privacy legislation and that standard.

Any of you can answer that question. Go ahead, Joey.

MR. WENDER: I'll take it. I'll speak on behalf of Congress, no problem. (Laughter)

Well, I would take your question and take it to the next level.

DR. TURNER LEE: Yes, yes.

MR. WENDER: The conversation is going to shift very quickly in 2020, and it's not going to simply be about California, but it's going to be about Washington State and it's going to be about Massachusetts and it's going to be about all the other states that start acting. So the world we're living in now is going to change very rapidly. And so it's not going to be, you know, as Cam accurately and on point recognized, that there's no way the House of Representatives would pass anything that was weaker than the California state standard given that about a quarter of their caucus is from California, including the Speaker.

The question is now going to be -- is going to become these laws are going to differ with each other. The California law will be different than the Washington State one or the Massachusetts one or the New York one or the Maryland one or whatever else it might be. And so how do we reconcile those differences, one? And then two, what does -- and the word -- I'm amazed that we're 38 minutes into this panel and the word has -- the P word has not been used yet.

DR. TURNER LEE: I was getting there.

MR. WENDER: Because that is the word, and it's preemption.

DR. TURNER LEE: Yes.

MR. WENDER: Preemption. What does preemption look like? Because let's just be honest with ourselves. Let's be honest. A lot of what is pushing, driving industry to want federal privacy legislation in the U.S. Congress is because they don't want to have to follow a patchwork of different state laws. They want the Feds to come in and preempt the states so that we have one national standard.

But, again, then it becomes what does that preemption look like? Not all preemption is created equal. Is it a ceiling? Is it a floor? How expansive is the preemption? How narrowly is it drawn?

And I guarantee that that, the extent of rulemaking at the FTC and what this private right of action will look like, it'll probably come down to those final issues on whether we can get final privacy

legislation across the finish line.

MR. KERRY: So one other thing that's going to happen in 2020 is that the dial in California-ometer is going to move. Because Alastair Mactaggart, the proponent of the referendum proposal that led to the adoption of CCPA, has a Version 2 in the pipeline. And that's going to come to the California legislature sometime in the spring, about the same time that the attorney general regulations that will raise the bar on the Version 1 are going to come into effect. So that's going to be ratcheting up.

MS. LAYTON: So, the gentlemen are absolutely right. This is going to be coming to a head, if you will, in 2020. I think the importance, though, to say is that many people just assume because it's government regulation that it's the voice of the consumer. And I would push back on that because what's really going on is it's an empowerment of government. Consumers have very different views about privacy.

And if you look at the way the California -- CCPA came together, Alastair Mactaggart made millions of dollars as a real estate guy using personal data to grow his business. And he didn't like the way Supercuts would collect your email whenever you signed up to get a haircut. Well, there are some people who happen to like Supercuts and they don't have a -- they want to get coupons and deals and so on. But it offended his sensibilities.

So the actual voice of consumers are very different and they're diverse. So I actually think the way through this is that we need to understand there's big tech, the large platforms. They're one order. I mean, we're talking about companies that are the size of -- they're larger than countries. It is very different than, you know, the run-of-the-mill ISP. It's very different than the church website or the school website or something you have in your home.

And I actually think we need to build the appropriate standards around that and have safe harbors so that we can evolve to a rational, reasonable world. We don't assume everyone's Google. I think that's ridiculous. But we're expecting, oh, my goodness, you know, Brookings, why don't you have, you know, these -- and then they're also, look at, you know, this challenge now because we're creating

asymmetry with government. Because you don't have the right to delete your data with government. Can you imagine going to the healthcare service and say I just want to delete my data now? How are you going to continue to get your healthcare insurance?

So there are some serious questions there. And I think what we need to kind of do is cordon off the concerns where the harm is, for example, platforms. It's very different than ordinary websites and other industries.

DR. TURNER LEE: Right. And so, Jeff, I want to come over to you because CCPA, though, assumes that all companies are the same. Right? That there is this assumption that compared to GDPR we are, I think, going to see in CCPA a lot of the definitions, a lot of the rules apply to every company, from the dry cleaner to the big tech company.

Is that something, in terms of compliance and, you know, will it cause any kind of regulatory confusion? Will there be issues related to that in terms of, you know, what data is for the -- I think, Roslyn, what you're mentioning, what's for the good of the consumer versus what's not? I mean, where's the confusion going to come when everybody's sort of put into the same bucket?

MR. BRUEGGEMAN: I think we may see some confusion in California next year. I would, you know, pick up on what Joey said, I think, but think about that multiplied by 10, 20 times if we get a number of other states acting. I think to their credit many states have taken a step back and said the California law is very complicated. There's high potential for unintended consequences. We're going to take our time and think through this. So I think there is a window to do something.

But, you know, the complexity will only grow if we have this patchwork of regulations. So think about almost any businesses online today, right, if I have to have a different user interface set of privacy terms, controls that are different depending on where my customers are located -- and, by the way, my customers move all the time and may have complicated relationships -- I think we're going to paralyze a lot of things, especially on the Internet.

So let's get this right. Let's have strong protections and let's have it be flexible enough so that whether you're a brick-and-mortar store or you're a tech company or you're a small business, you

know, again, if we do this right, we want to be sure that privacy protections apply across the board, but we need to not be so proscriptive that you can't accommodate that variation.

MR. KERRY: Yeah. So CCPA does have a carve-out for small businesses based on the volume of business or the number of records that you have. And that's something that was adopted in the Democratic bill in the Senate. And I think an across-the-board carve-out is maybe too broad because anybody that collects data should at least be thinking about privacy and have some obligations to handle that data appropriately. And actually, the Wicker bill adopts that approach and then carves out certain obligations. So the access correction, et cetera, obligations, you know, there's a carve-out.

And those are the ones that really have the significant compliance costs. I mean, all the back-end process of designing the consents, designing the portals, having the capacity in the company actually to turn over those records. That's where the real effort comes in.

DR. TURNER LEE: So I want to take questions in just a few moments. If you have a question we'll come out and actually have my friends here and colleagues at Brookings help us to direct those questions. I do want to ask this final question of this panel of something to think about.

So I started with the sandwich model: GDPR, CCPA, in the middle the meat, if you're a vegetarian the tomato, could actually be federal privacy legislation. Right? Which takes the good of each side and adds a little bit more flavor to it or perhaps it's so flavorful, like a pastrami sandwich, that it just dismisses the bread. Right?

We've talked about process, compliance, enforcement, covered entities, discrimination, legal recourse. I'd like to hear from each of you where will we land up on federal privacy legislation given that? Which of these areas will we have to do a little bit more discussion on? What are some areas that you may want to do better definition? But, you know, I think that both sides of the sandwich gives us something to work with, I think is what was mentioned earlier.

Cam?

MR. KERRY: I don't know, I think I got a mess on my face at this point. (Laughter)

DR. TURNER LEE: And in what area? Like out of all things that have sort of come up on

the bread, what should we be focusing on next?

MR. KERRY: Well, look, there's obviously a big gap on both preemption and private right of action. I think that those things kind of work together, but, you know, you get one national standard that provides strong protection, so building on what's there in terms of the limitations on collection and use and retention, sharing of data.

And some forms of strong redress, we're not sure that that's going to likely wind up being a broad private right of action and it brings the class action bar in as a force multiplier. But I think that there is a path to get there and that's, I think, the project of the next three or four months.

DR. TURNER LEE: Okay. Joey?

MR. WENDER: I agree with all that. I would add two other issues.

One is, again, what are the use limitations? Are we going to prohibit companies from sharing or selling your biometric information? You know, it's been said if somebody steals your Social Security number, you can apply for a new one. But if someone steals your facial image, you can't get a new face. You could try, but you can't get a new face. That was a joke, guys. You're supposed to laugh. (Laughter) Thank you.

DR. TURNER LEE: I was going to say, you can't get a new face.

MR. WENDER: Right. There's a sandwich metaphor there. (Laughter) So I would say that's the first area that there's going to be a lot of discussion on what are those use limitations?

The second is, and this is contemplated in both the Cantwell bill and in the Wicker bill, is are we creating different regimes for sensitive versus non-sensitive information? What is sensitive? What is non-sensitive? What applies? That's a very complicated conversation, particularly when it's recognized that the universe of sensitive information online is only increasing, so you don't want to have a static definition either. Or do you not even use that paradigm altogether and you just have -- you really just have an exception for information that is transmitted in the course of a transaction versus everything else?

So I think those types of questions are very real, they're very current, and I don't think

there's a -- it's not clear what exactly the answer should be right now.

MS. LAYTON: So I'm ultimately optimistic that the process will pay out in the right way, particularly because I see where we are is a part of -- been a long journey for America where we have had this interplay between the states and the federal government and interstate commerce. This is an issue going back to the Constitution. So these things have been there.

The two areas I think that will come to a -- will have more to play in 2020, one will be the Uniform Law Commission. This is a group of state-based actors who are working together. I mean, in addition to Congress, we have all kinds of state-based actors who are trying to resolve the differences in states because they, too, see the importance of maintaining valuable, seamless Internet economy that we have. So that will be there.

And by the way, this is more than the Europeans ever did. They did not have these levels of discussion and detail, every state working in that way. So I'm even more encouraged because of the quality of the discussion.

And then the other part I'd say is we can take a better look at independent certifiable standards. These are privacy-based standards, security-based standards that are developed in independent institutes. We're not relying on someone's subjective definition. But those can also resolve a lot of the questions that we have where people want to say it has to be this say, but we could look at how a standard's written and then map our technology to the standard. And I think that that will help us in some of those places where we have an impasse.

And then my hope is that Congress will also think about safe harbors because a lot of companies, they want to do the right thing. They don't have millions of dollars. They want to get there. They need time to do it and then I think that our lawmakers will be -- they'll see that that's going in the right direction and adopt a sort of safe harbor to allow companies to evolve.

DR. TURNER LEE: Jeff?

MR. BRUEGGEMAN: So we've kind of looked back on this panel of how did we get to where we are, but I think in privacy legislation we also need to look ahead. And we're on the cusp of AI,

machine learning, and incredible uses of data. And I think there is a -- you know, we may not address all of those issues at this point, but we certainly need to be taking account of them and we need to be thinking about how we protect consumers and stop behavior that we don't want with data while not being so restrictive that we don't enable those exciting new services. And I think if we do that, we actually will have an advantage globally in how we address privacy.

And then the second issue, back to Cam's point, enforcement, I think it's underappreciated component of privacy legislation is how much this is strengthening both the FTC's enforcement and state enforcement on privacy; new fining authority, you know, just regulatory authority, and stricter rules that are going to make it easier to enforce.

And so I think when we talk about issues like private right of action, we should do it in the broader context of let's look at the overall picture and make sure consumers have remedies and that there is strong enforcement. But that is a broader set of requirements that are in these privacy bills.

DR. TURNER LEE: And I would say, you know, moderator privilege before we open it up, I think all of what you have said is correct, right, in terms of where we're going to go on this trajectory. I think it is important that we look at machine learning and AI as sort of a separate conversation because of the technological nuances. But I think in privacy legislation, on the discrimination side, which I think GDPR has covered this, and I know California will go even deeper, discrimination is purely wrong, whether it's online or offline. So I think there are easy fixes to actually ensure that the statutes that exist today apply to privacy legislation.

But I do want to keep going back to compliance. I mean, I think there's also this issue of how do you not create a patchwork, what you're saying, still give strong state authority and jurisdiction while not having privacy attorneys become richer? Sorry some you attorneys out there. Right? (Laughter) This is really going back to the base of the problem that we're trying to solve and not the one that we're trying to create.

So with that, and I had to ask, you know, I couldn't sit here, the last panel of the day and not say nothing, I'm sorry, everybody, but I feel I got to be here. I want to ask questions of the audience.

So I'm going to start from the front and lead to the back. We've given some time. I'm glad to see a lot of hands up. Let's start with this young man right here and then we'll switch over to my dear friend here, and then we'll move our way back. Okay.

Just say your name and direct your question. I'll as that these be questions and not commentary so we can get everybody in. And the panelists will respond accordingly.

MR. COLEMAN: Richard Coleman, retired from Customs and Border Protection when it was called the Customs Service and before that the Bureau of Customs.

One of my jobs was answering Freedom of Information Act requests and Privacy Act requests. The government was limited on what it could collect and how it could disseminate information. All that was in the public interest of a law enforcement agency.

I can't get my brain around the idea that corporations should be allowed to get your personal data, which is not in the public interest, buy it and sell it, and the objection that it would be too costly to change presumes that the default position as they get to keep the information. I think the default position should be they don't get to keep the information unless they can justify that it's in the public interest.

And the idea that there's a cost-benefit analysis, Americans With Disabilities Act, what's the cost-benefit of that? The civil rights legislation, what's the cost-benefit of that? Doing the right thing, what's the cost-benefit? It just doesn't make sense.

DR. TURNER LEE: So you want to make that as a comment or a question?

MR. COLEMAN: Either way.

DR. TURNER LEE: I thought about that, but we've got a little bit of time for me to do one, Roz, because I'm trying to make sure I keep my focused attention here. So I'll treat that as a comment. Okay? You all heard it? I think that's why we're trying to pass federal privacy legislation, so I think you're right on point with that.

Let's go to the next question.

MR. SCHRADER: Hi, Paul Schrader. Thanks, Nicol. So three quick things, I guess

questions.

So one is I work for a startup serving people with disabilities where maintaining and holding data could actually be really helpful for our customers. I worry, though, that often in these cases it's companies like ours that pay the price when the elephants are fighting: Facebook, Google, et cetera. We're the ones that get stomped on by government action potentially. So how do we protect startups doing good things, but also ensure that startups that could be doing harmful things aren't allowed to do harmful things?

And then the thing that surprised me that you didn't talk about is revenue models. So consumers expect and love having free Facebook and free Google Search, but there's a cost to that. And the cost to that is advertising and targeted advertising and we see where that goes. So how do we deal with that?

And then finally, enforcement penalties, I'm really surprised you didn't talk about that and whether we need a different regime for enforcement penalties. Many have complained that the FTC findings -- enforcement have been far too low on the companies where they have found fault.

DR. TURNER LEE: Paul, thank you for that. We're going to have more events, so we'll talk more about that.

All right, go ahead, Roslyn.

MS. LAYTON: I want to thank you for that question. And if I haven't mistaken, I recall you testified in Congress on a prioritization hearing. It was a brilliant example of how technology can be used for good and the importance of when we have this kind of one-size-fits-all about how we treat the Internet that we will eliminate important services such as yours and how you are -- you can get assistance walking across the street. So anyway, I so appreciate that you're here and that you're involved in this debate, and you made so many good points.

On enforcement, take an example of the FTC with Facebook, this $5 billion settlement. That's $5 billion, 200 times more than we have ever had for any privacy settlement in the United States, and it's 20 times more than what Facebook would be charged in the European Union under GDPR. And

by the way, that was done in less than one year with the existing resources at the FTC and without any new laws.

So we don't know if anything will ever come to pass with Facebook and the European Union because Facebook will probably sue them and they can't ever get that much money. So I think that that's worthy to look at in terms of what the FTC can do today and all of the legislation talks about strengthening the FTC. So that is one area.

The other thing is the restrictions now on Facebook as a result of that settlement actually go beyond the GDPR in terms of the personal certifications Mark Zuckerberg has to make to the FTC every single quarter on pain of not death, but criminal penalty, he can go to jail, as well as the chief privacy officer. So if anyone doubts that the FTC can't step in, they can and that sends a signal to business.

I also think what's good about that is that we haven't saddled every company with the same obligations as Facebook because they haven't done anything wrong. But this was a case where the harm needed to be remedied and FTC stepped in.

So I guess the other thing that you're -- I'm not going to take all the time. I just wanted to make that point. I'm sure the other panelists can --

DR. TURNER LEE: Anybody else want to comment?

MR. KERRY: Yeah, just two quick comments. As has been pointed out, all of the bills would strengthening the fining authority of the FTC and allow it to issue fines in the first instance, which it could not do in the Facebook case.

And secondly, I think in terms of dealing with the beneficial uses of data, I think it's important to focus on sort of a general duty of fairness. This is something that I think the bills are getting at and still struggling to find exactly the right formulation. But to really -- you know, companies talk about being data stewards. And I think that is the key goal is to make people good stewards of data. And the good steward puts the interests of the principal ahead of their own.

DR. TURNER LEE: Okay, I've got time for one more question. This gentleman over

here giving me eye contact.

SPEAKER: Good morning. And Nicol and Brookings, thanks for inviting us and all. And my question really is going to go to Joe.

As a data standard setting body in education we support a federal standard. But there has to be an educational piece to that and I'm wondering if there will. And the reason is I actually don't think there's going to be a sea change from the consumer perspective because Americans are blinded by the word "free." And it is a fraudulent use of the word. And unless there's something in there, Americans are going to see "free" and not care and click the box and all this is going to be in vain.

But will there be something in legislation about education and about -- I mean, credit reporting agencies, do consumers know how credit reporting agencies work?

MR. WENDER: So the answer is we hope. I mean, we obviously want to have an educational piece to this. And what I would say, this is the whole challenge that we're having right now in many ways, is that people do like these companies. Right? They like the fact that they're free because they don't have to actually pay a dime up front for it. And they always work and, as the previous gentleman said, people like targeted advertising. Right? These are things that people, for the most part, that people like. They help drive the economy and help get people what they need.

That being said, if you watch the polling that's being done, there's more and more awareness amongst the American people that, wait a second, there's a sinister side to this. What am I giving up? I mean, the first gentleman whose comment who I agree with, you know, and this has been asked of Mark Zuckerberg when he was before the Senate Commerce Committee is that who owns your information? Right? Who owns it?

Obviously, we believe that the consumer continues to own his or her information and that privacy is a fundamental right. But how are all these things balanced and how is all this information explained consumers? I think that's the challenge that we have right now in writing this large bill.

DR. TURNER LEE: So we've run out of time. So I want to offer you a couple of holiday presents.

First, our panelists, let's give them a round of applause. (Applause) You can find each and every one of them on the Internet, so please continue this dialogue through the #PrivacyDebate or directly to them.

And then I'm going to give you two more holiday presents before you run out of here. The second one is the series that we have at Brookings called The Privacy Debates run by my colleague Cam Kerry. We're all invested in the dialogue around this and I encourage all of you to look at a recent blog that he put out a couple weeks ago, in addition to the information that we'll be sharing from other scholars.

And then the third gift is our AI series here at Brookings. We have a broad institutional AI focus which is looking at governance, bias, and national security. Right now on the Brookings website are a series of papers around governance, as well as on bias. So I also offer that to you for free to visit our website and look at that.

I just want to say thank you all. This was a really important conversation to have as we go on the eve of the next decade into the passage of the CCPA. So let's keep talking because I think what we learned in this conversation is there's more to be done. Thank you very much and have a good rest of the day. (Applause)

Oh, before I forget, this is new. Fill out that darn paper, please. And leave it with one of our Brookings staff and colleagues in the back. Thank you very much.

* * * * *

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