THE BROOKINGS INSTITUTION

THE FUTURE OF ONLINE PRIVACY: TO LEGISLATE OR NOT

Washington, D.C.

Thursday, July 26, 2018

PARTICIPANTS:

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

MELIKA CARROLL
Senior Vice President, Global Government Affairs
Internet Association

NUALA O'CONNOR
President and Chief Executive Officer
Center for Democracy & Technology

KAREN ZACHARIA
Vice President, Deputy Counsel, and Chief Privacy Officer
Verizon

* * * * *

P R O C E E D I N G S

DR. TURNER-LEE: Hello, everybody.

GROUP: Hello.

DR. TURNER-LEE: Good afternoon. So I see a whole lot of people had something really important to do on a Thursday afternoon. Thank you and welcome to Brookings.

My name is Dr. Nicol Turner-Lee. I'm a fellow in the Center for Technology Innovation here at Brookings, located in Governance Studies. And my particular portfolio is on regulatory legislative policy in addition to digital inclusion. I have a book coming out in 2018 on digital inclusion. And I also work on automation algorithmic bias in AI.

So happy to facilitate this panel with, first of all, if we can acknowledge these all women that are up here. (Laughter and applause) It was not by intent, but it happened by design. They are actually going to speak about this topic and I'm really excited because I have a relationship with all of them. And this is a timely topic. I think all of you through your demonstration of being here today actually are talking and thinking about this topic, so our hope today is to really flush out and unpack what the conversation has been generally and granularly. What should we be thinking about as we move towards some type of legislation framework when it comes to privacy?

So we made this timeframe quite short because we're going to skip the formal introductions and go right to who these wonderful ladies are and we're going to jump right into the discussion. As with any Brookings event, we do have a hashtag, #OnlinePrivacy, that if you are going to tweet we'd like you to actually use that. And we will reserve the last 15 to 20 minutes for question-and-answers. So let's get started.

Right here next to me is Karen Zacharia, who is the vice president,

deputy counsel, and chief privacy officer at Verizon. At Brookings, we do believe in transparency, so we would like to share that Verizon is a donor to the Center for Technology Innovation.

Seated next to her is Melika Carroll, who is the senior vice president, Global Government Affairs, at the Internet Association.

And next to her, my friend and my goal partner, Nuala O'Connor, who is the president and CEO of the Center for Democracy and Technology. Let's give them a round of applause for being here. (Applause)

All right, ladies, I'm going to start with this first question and then let's sort of use this as your way to sort of talk through what you've been thinking about when we talk about to legislate or not privacy. Let's start with this. Should the U.S. be looking at privacy legislation? Let's sort of put that to bed given some of the concerns that have arisen around online consumer privacy.

So, Karen, I'll start with you.

MS. ZACHARIA: Yeah. I mean, my answer is absolutely. I've been fortunate enough to be in this role at Verizon for seven years, and in the seven years that I've been in this position Verizon has thought there should be federal privacy legislation. And our main reason for thinking that is that we think it's really important that consumers have a baseline trust in the system. And one of the really easy or best ways to get there would be to have federal privacy legislation. So yes.

DR. TURNER-LEE: Yes. Okay, we're going to go down, too, we'll get a little deeper on what that looks like.

What about you, Melika?

MS. CARROLL: Yeah, we think it's a very important conversation to have. You know, when we think about the Internet Association the companies represent,

our companies provide a lot of tools for users to set their privacy preferences. Right? But there's also a big conversation about improving consumer trust and that, at the end of the day, is our top priority. And so when we think about federal privacy legislation we're thinking what are the goals we're trying to achieve?

You know, one is, and the foremost is, how do we ensure user trust? The other on is, you know, from a broad perspective how do we ensure innovation and ongoing development in technology? And then finally, as we think about federal legislation, too, how do we think about regulatory interoperability, right? How do these frameworks work across state lines, national borders, et cetera?

And I think the other thing we're thinking about when we discuss federal privacy legislation is that it's not a tech issue or an Internet issue. Right? Data is an issue for every part of society and the economy. It cuts across tech, transportation, real estate, whatever the industry or nonprofits or government might be, right, everybody has an interest and every user has an interest in data.

DR. TURNER-LEE: Yeah. Nuala?

MS. O'CONNOR: Well, first of all, thank you to Nicol for putting together this great panel. It's just fun to be with friends to talk about something we've been talking about for actually several decades some of us.

It will surprise no one that I personally and the Center for Democracy and Technology have long espoused and advocated for omnibus federal privacy legislation in this country for, frankly, many of the reasons that Melika and Karen already said, but, first and foremost, for the rights of the human being in the digital age. As our data becomes more fluid and more global it is hard for any one individual to know and fully understand all of the ways it's being used, who's got access to it, how it's being captured and

analyzed. So I always like to say it's not just the data, it's also the decision that matters, the decisions that are made about you in the digital world in infinitesimal time.

We're excited about the promise of innovation and AI and the Internet of Things and the Internet of Everything. I also say that it's the Internet of People first and foremost to us. But how we exert control over our own data, I mean, the old adage "Knowledge is power" is true. Data about you allows you to be known in certain ways and decisions be made about you. So we really believe that issues of equity are best solved and issues of transparency are also solved in a baseline federal privacy legislation that, as Melika said, is not just for the tech industry. It's for any industry that has data about human beings, but it also feeds into the global dialogue.

I mean, I think this is also the perfect storm. It's not just should the U.S. be considering it? It is. I mean, we're talking to dozens, literally dozens, of members of Congress right now about different ideas they have. And this plays into the perfect storm, frankly, of GDPR, California, and Cambridge Analytica. So we're seeing people at the table that have not been at the table in two decades.

DR. TURNER-LEE: And so I want to actually -- and I love the analogy of the perfect storm, so let's talk a little bit about I think the U.S. always thought we were going to be first. But the GDPR sort of beat us to that, right, in terms of at least putting out a framework. And now we see the state of California with their own Data Privacy Act. So I want to talk a little bit about that.

I mean, is that going to sort of forestall our push towards U.S. privacy legislation? Should we be taking cues from GDPR, taking cues from California? I mean, if we can let's start there first, just higher level. Now that there's been some precedent set, what do we do about it in this discussion around U.S. federal privacy legislation?

MS. O'CONNOR: Start with me?

DR. TURNER-LEE: Yeah, let's start with you.

MS. O'CONNOR: Okay. So we actually did not formally endorse the California legislation. We think there are issues with it and certainly there are challenges with GDPR, not the least of which is that it's not entirely clear how some of the provisions are going to be enforced.

I do think, though, you see a thread of principles and they date back, frankly, as we were discussing earlier, to the Obama administration's Consumer Privacy Bill of Rights, but even further back with the Fair Information Practice Principles. I think there are global ideals in the Human Rights Directive and elsewhere of dignity, of human dignity, and what the boundaries are around you and your continuing control or at least kind of relationship to your own data.

I don't really like the construct of ownership. I never thought -- we look at (inaudible), as you know, as a property right or something of a property right. As we kind of overly generalize the Europeans look at it as a human rights issue. But I look at it as kind of an extension of self. Right? What is the digital self? What is your habeas data, as has been recently written about? And what is your continuing ability to control that data about you in the digital world while also engaging with companies or other human beings online?

DR. TURNER-LEE: Melika, you want to step in?

MS. CARROLL: Sure. I mean, from our perspective, obviously, you know, we're very aware of these other rules and how the discussion is progressing in in other markets or jurisdictions, but we really feel strongly that we should have a separate approach and a unique approach to the U.S. federal system.

You know, privacy, all of us know who have done this for a while, is very cultural. Right. The Canadian political system and privacy requirements are different

than the (inaudible), et cetera. And there are a lot of unique characteristics both about our own political system and regulatory environment and, frankly, our own economy that we want to preserve and protect. And we think we should come up with our own federal system.

DR. TURNER-LEE: Karen?

MS. ZACHARIA: You know, I think about what privacy legislation should look like a little bit like being in the middle of a really complicated maze. And there might be several different routes to get to the end goal and it doesn't matter -- you don't have to find the perfect one. What you have to do is find one that gets you to that goal.

And so when I think about privacy legislation and when I read a new bill I look for four things. The four things are we need a national framework. The Internet doesn't stop at state boundaries, so we really need something that covers the whole country and isn't state-by-state.

We need something that's consistent, meaning that all the players have the same rules. And I think this is really important from a customer's perspective because when a customer thinks about their information they don't think is my location information going to an app provider? Is it going to social media? Is it going to a telecom company? They think I have location information and I want it protected.

I think it needs to be flexible. Technology is changing so quickly and in ways that we can't anticipate that we need to make sure that whatever the law says is going to cover us in 2 years, in 5 years, in 10 years.

And then last, it really should focus on what's most important to customers. So if we end up with a law that's highly regulatory, but has the effect of having consumers saying I accept, I accept, I accept, I accept, I accept, you know, that doesn't really advance the goal here. It doesn't move the needle. And instead, what we

should look at are the things that are most important to customers or consumers, you know. What's the most sensitive information? What are they most concerned about? And then put some special rules around those.

DR. TURNER-LEE: So I want to -- I've been taking some notes. There's been so much on the table. Right? So I want to go back to and then kind of unpack, I think, this platform piece in terms of the application to everybody.

So, you know, GDPR may come with some constitutional challenges. It's hard in the United States. I've been telling people you look at the formation of the Internet in the U.S., Clinton and Gore made a deliberate decision to make it a reciprocal marketplace. That's now Europe uses data. Plus this was six years ago, it's just getting implemented. So we can maybe reserve some time for that.

But California's interesting. I mean, Jerry Jones, that's a big state, who actually has outlined this relationship to data. And if we move forward with a national framework, preempting the entire state could be problematic, right? Or it may not actually preclude us from actually having other states follow.

So I'm just curious, and for those of you, the California privacy act won't go into effect until 2020, but it's pretty much a relational definition of how people should have data. I should be able to delete it. Businesses should tell me what they're doing. It's the basic principles of Obama.

Again, I want to just kind of ask this question. Should we be paying attention to that or is that something where we should have California sort of become part of the conversation, so we avoid what Karen is talking about, the state-by-state legislation? That's for anybody.

MS. O'CONNOR: Well, I think we are paying attention to California and I think we should. I'm mindful of the march of state laws on data breach and how that

happened. Right, it did take, what, 15 years or more from the California law to the last state to pass data breach.

And I'm also mindful, I think Karen makes an excellent point, a patchwork approach at the state level or even globally is not good for consumers and it doesn't reflect the way data flows. It's not a realistic framework and it stymies and impedes innovation. And also, it doesn't support what the individual expects, that they are certain about where their data or at least what rules govern their data.

So I do think there are going to have to be boundaries on kind of what's in, you need to know where someone -- the example I always used to use and then I worked at Amazon and I now don't and I'm going to use the example again, is Amazon needs to know where you live in order to deliver the book. Right? That seems to be essential data for that transaction. Right? The further away you go from the primary purpose, then I think you become more and more attenuated from the individual's expectations about the data use. And so there are things that are going to be in the bucket, in the obviously used.

There might be things that we decide as a country based on our cultural norms or on our legislation demands that are simply out of bounds, right, whether it's I'm not going to use DNA in hiring, right, or something really outrageous and kind of irrelevant to a transaction at hand. And then there may be things in the middle that require different levels of notice or different levels of kind of consent.

I don't think that the conversation -- please, let's all move beyond opt-in and opt-out. Like that was so 20 years ago and I am so tired of that conversation. (Laughter) And it's even moving beyond just simply notice. How do you give notice of sensors that are on the street as you're walking by? Or how do you give notice in kind of the real-time ubiquitous collection of data? I think we've got to be really creative.

And again, I will commend my former employer for things like the lighting up on the Echo and other devices that are interactive and use non-alphanumeric disclosures as you go about your day. So I think there's opportunity for creativity in the tech sector and elsewhere in engaging people with the technology in their daily lives.

MS. CARROLL: And I think what you're hearing here and we would agree, this is really complex, right? And at the end of the day we want a system that, again, promotes user trust and that is comprehensive across the board, that takes into consideration different uses, different types of collection across industries and sectors. And you can't do that over a few days and you can't do that with a very narrow set of people having conversation.

And so, again, I think, you know, California happened in the way it did for a very set of specific circumstances, what you're starting here with a conversation with us. And I think what you're hearing is agreement on a lot of broad principles, but that requires conversations with a lot of different groups in different sectors of the economy and, frankly, NGOs and other stakeholders.

DR. TURNER-LEE: Karen, do you want to just jump in on that one or do you think you said your piece?

MS. ZACHARIA: I think I said my piece on that. (Laughter) I'll just agree with what they said.

DR. TURNER-LEE: So I want to actually then pick up then the second point of this whole universal application of federal legislation to all companies. Are we in agreement there or is that something that we still need to sort of tackle and granularly look at?

I mean, Melika, I'll start with you.

MS. CARROLL: Sure.

DR. TURNER-LEE: Are we in agreement there?

MS. CARROLL: I think we're very focused on what is the consumer, again, right? And let's look at the data and have a risk-based approach. Some types of data are very important, very personal. Some types of data are absolutely not. And if we have a system that treats all of it the same way, whether a light goes on or off, the same as whether I walked into my doctor's office, that's going to be not very effective for most people and, in particular, the user.

And so we feel that one system is important to kind cross across sectors. Right? The user is not thinking am I shopping in the store or am I shopping online? They want their data to be treated the same way. But we have to be sensitive or recognize that there different types of data that are being collected.

DR. TURNER-LEE: Karen, you want to jump in on that one?

MS. ZACHARIA: Yeah. No, I mean, I agree on both points. I think you have to both focus on the data and how sensitive it is and whether you're talking about turning on a lightbulb or going into a doctor's office. That's, you know, good. We generally think about location information as being very sensitive and other things are less sensitive. So I think that's definitely one aspect of this.

And then the other, you know, as I said earlier, it doesn't really matter the type of player who's collecting it. The same rules of the road should apply.

MS. O'CONNOR: So I first saw this when I was at the General Electric Company, the once great General Electric Company, which had 11 different divisions, including aviation and nuclear power plants and trains and all sorts of things, and several banks by the way. And every sector had different regulation and every sector had different rules and expectations about how the exact same data element would be treated. And then they'd want to cross the streams, basically. And I'd say you can't do

that because you collected it under this regime and it's not going to work under that regime.

So I do, first of all, want to answer the question I think every sector should be covered because data is data and it's flowing madly and wildly, hopefully for the public good, but that's an open question. And it would be unfair to either privilege or disadvantage any one particular industry or sector.

I do think there are elements, and I'm going to mix it up a little bit because we're in such violent agreement on this panel that I'm going to just --

DR. TURNER-LEE: Thank you. (Laughter)

MS. O'CONNOR: Trust me to be the bomb thrower, as usual.

DR. TURNER-LEE: That's unusual, Melika.

MS. O'CONNOR: No, not at all. (Laughter) Anyway, but yes, sensitive data. And yes, I have a particular bête noire about location data. But, you know, I'm mindful of the recent revelations of the Cambridge Analytica kind of issue. And I think the ah-ha moment there was we've always known in the data science world that data aggregation and trivial data could be triangulated to not only locate you, but to make inferences about you in the real world.

I think this set of allegations of incidents kind of awoke the general public to the idea that trivial data, data like what's your favorite color or what kind of dog breed do you have at home, can suddenly be used to be aggregated and make decisions and inferences about you that not only serve you advertising -- again, everybody's all up in arms about advertising, advertising fuels many parts of the Internet, let's not forget -- but to make consequential decisions about what you see and thus what you experience in your world possibly up to and including political decision-makings or knowledge of your citizenship, of your society and your democracy.

And so while I agree that there are certain kinds of data that require extra kind of white gloves, you know, kid glove treatment, I think that large-scale data aggregations, sometimes even in the anonymized or de-identified space, can have very, very serious consequences for the fragmentation of the society. And another area we work on at CDT in addition to data and privacy obviously is free expression and kind of the creation of community. And I'm deeply concerned about the inferences and the decision-making that drives from arises from, again, trivial data and seemingly entertaining and fun data about individuals.

DR. TURNER-LEE: That's right. Well, I mean, the work that I'm doing on bias and what Helen Nissenbaum has talked about, it's the institutional societal consequences of that that makes my very innocuous purchase of red shoes translate into a different message, which I think is a harder thing to legislate. I have to be honest, that it's not that easy, you know, because you also have to get policymakers to also understand this ecology and they don't. Right?

MS. O'CONNOR: Care about the outcomes. Right?

DR. TURNER-LEE: Yeah, yeah.

MS. O'CONNOR: And you can test for outcomes and we have a tool. I'm going to promote CDT's website again, called Digital Decisions, that people -- companies and institutions of all kinds can plug in their kind of factors and values and algorithmic decision-making to ferret out what we hope is unintended bias.

DR. TURNER-LEE: Exactly.

MS. O'CONNOR: But that doesn't help them build from the -- you need to build against and ferret out that bias from the beginning of that kind of software development, the life cycle of the algorithmic decision-making process.

I have a new theory and a new theme that I'm kind of working on and I'm

going to share it all with you. You can all take it for what it's worth, and that is it's the inherent architecture. It's not even just the data, but it's the inherent architecture that reflects the bias of the creator. I'm particularly down on one online fora that I will not name that I think reflects a particular race and gender's way of speaking to each other and that privileges that group over groups and other ways of communicating.

DR. TURNER-LEE: So I'm going to just translate that for you. (Laughter) Sorry, Melika, there's no diversity in Silicon Valley that actually has checks and balances. I mean, there's no diversity in design. That's actually another panel, it's another paper that I have coming out in the fall.

MS. CARROLL: But I do want to touch on that. I think the diversity problem is a really important one.

DR. TURNER-LEE: It is an important one.

MS. CARROLL: And it's important across almost every sector, both women and diversity and gender diversity and -- sorry, gender diversity and ethnic diversity. And it's something that we've recognized and I think all the companies are working on. And, frankly, we were the first trade association to hire --

DR. TURNER-LEE: A chief diversity officer.

MS. CARROLL: -- a head of diversity.

DR. TURNER-LEE: That's right.

MS. CARROLL: And the role is really important because it's not just to have relationships with diverse caucuses, right? It's really to work with the member companies to develop programs, do benchmarking, and best practices so that they can learn from each other and try to change the dynamic at every level, not just having more diversity officers, but having diversity in the programming team. Right? So something we recognize.

DR. TURNER-LEE: No, you're right. No, no, and I think we can agree that you all are working on this, right?

But there's so much more work to do on this.

MS. CARROLL: Absolutely.

DR. TURNER-LEE: But that's another panel and I'm actually not going to open that one up because then we're going to be talking about a federal legislation for privacy. But I do want to actually talk about it because I think this conversation sort of is now the emerging dialogue and the U.S. has sort of been locked into this patchwork of federal and state policies with a focus on data breach. Right? And we couldn't even pass national data breach legislation, if we wall recall.

Will there be -- and I want to unpack now what actually should be in this federal legislation. It's clear that it should probably move more towards based on what you all are talking about, the relationship with data, data use and collection. But what about all of the stuff that we worked on around national data breach policy? Is this a possibility of actually getting that done? You know, will we see opt-in/opt-out survive in this legislation or is it something that we should recreate something different?

I'll kind of go down the line. I'll start with you, Karen.

MS. ZACHARIA: Okay. So I'm going to take the data breach question first. You know, we also think that there should be federal data breach legislation. Whether that should be part of the same package with privacy legislation or not, I think from a policy matter it probably doesn't matter. I think the real question is a strategy question. And honestly, I'm going to leave that to people in Congress to figure out. You know, I think we need both. And whether we do them together or separately, you know, other people can help figure that out.

In terms of the specifics, though, you asked about -- what was --

DR. TURNER-LEE: Opt-in/opt-out.

MS. ZACHARIA: Opt-in/opt-out.

DR. TURNER-LEE: Should we still be looking at that?

MS. ZACHARIA: You know, I think I come back to what I said in the beginning, there are many different paths to get to the end goal here. It could include opt-in for sensitive information. That's certainly something we've supported before, but I don't think that's the only way to do it.

DR. TURNER-LEE: Melika?

MS. CARROLL: Yeah. I mean, we're still having this conversation with the member companies about what we would like to see in federal legislation. But at a high level we've supported data breach, data security legislation before. I agree, it's a question of kind of politics and process.

You know, I think data security is a very important part of data privacy. You can have the best privacy rules in the world, if the data's all out in the clear and it's not protected that's not very useful either. So there's a very good policy and substantive case to make to have them both move together, but we want success, I assume. And so, you know, whatever the best process is to enable that, yeah.

DR. TURNER-LEE: Yeah, that could work.

MS. O'CONNOR: So we have data breach laws. Is it now 50 or is it 49? I think it's 50 states.

DR. TURNER-LEE: Fifty.

MS. O'CONNOR: So I kind of wonder do we really need a federal standard at this point because we've got so much? But, I mean, to the extent it could be harmonized in a good way, sure.

And, of course, Melika makes the excellent point that security is

fundamental to privacy. We wouldn't want to see a chilling effect on innovation and security by saying you have to use X, Y, and Z. But we would want to see kind of a standard of care, right, a duty of care.

And that's where I would pivot into the information fiduciary space, which has gone in a lot of different directions. I think of it in the sense of being a custodian, that you when you're holding data as part of a commercial transaction or kind of in agency for an individual that you have some duty of care to keep it safe and to use it for the ways that it was intended or was part of the initial bargain or kind of within the zone of reasonable bargain with the consumer or the individual. But I'm curious about that and I'm kind of watching it. It could be taken to an extreme, but there is some sense of a larger custodian or kind of agency model for the commercial entity that is holding data on behalf of an individual.

And then I think we get to issues of unfairness and how do you legislate that. And we have an unfair and deceptive standard at the Federal Trade Commission and we have -- you know, we're looking at laws like the Fair Housing Act and the CRA and the FCRA and looking at where have we gotten this right in kind of a limited, targeted, tailored way. And you're right, we also, again, have the First Amendment side of the House saying no, no right to be forgotten, none of that stuff. Right?

But I will say, again, when we paint U.S. or EU in broad brushes we get it wrong. Right? I mean, culturally or legally. The United States has a right to be forgotten and it is called the Fair Credit Reporting Act. Right? And having just bought a house we all know I'm very intimately aware of what's on my credit report right now. And you are forgotten. You are forgiven and forgotten for different kinds of financial transgressions at different numbers of years.

We've decided as a culture, as a society that in the financial services

world you have a right to be forgiven and to begin again. You have a right in certain states as a juvenile offender to be forgiven and begin again. These rights to be forgotten are very sectoral and it reflects the traditional U.S. sectoral approach to data and to dignity and to privacy.

And so I would just say, I do it all the time, I generalize, oh, the Europeans. The Europeans always remind me, oh, no, no, no, there is no Europeans. There's French maybe or German or maybe even sectoral even within the country. So there are wide ranges of expectations. I think the first step to showing dignity for your customer or your consumer or your fellow citizen is being transparent. That's a necessary but not sufficient first step. And then talking about are you doing what is right and fair?

DR. TURNER-LEE: Right. So this is interesting because I think, again, this is scary, there's still some overwhelming agreement on the fact that there should be a framework that pushes out transparency, you know, something on security potentially, sort of resolve this data breach piece if we can, bring in some type of structure. But what's interesting about this debate is that there's still under the 2012-2015 Obama "Rules of the Road" this value proposition that comes with that, which is where I think the information fiduciaries come in. My colleague, Cam Kerry, just wrote a really good paper around privacy sort of dating back to what happened with the "Rules of the Road" and whether or not we should be actually using those.

But one of the challenges that we do have in the United States, though, is what is the FTC's authority? I mean, last week the chairman of the FTC, the Federal Trade Commission for those you who don't know, testified they have no rulemaking authority. So it makes enforcement quite difficult without that.

What do we need to do in the United States, let's say we put this

legislation together, to empower the FTC to be the cop on the beat? Is it going to be possible without rulemaking authority? Should we be thinking of another model to sort of help them enforce what I think we think of as values as well as statutes or other laws or regs?

MS. O'CONNOR: I'll start, sure. I feel like I'm talking too much. Cam and I go way back and we share that vision very much that, you know, one of the differences in the U.S.-EU framework right now is the ex ante versus ex post enforcement. Right? And I'm beginning to kind of very much believe that maybe the ex post enforcement doesn't work in data, right, because once it's out and the harm has been done, it's too late. So we are definitely looking at and exploring ideas of increasing both the footprint of the FTC in terms of what it covers and then increasing the possibility of some rulemaking.

I mean, we do now work in front of the FCC and the FTC and I'm curious about the differences in those agencies and how they've evolved. But I do think some more guidance, again, serves both the companies and the individuals of creating certainty and kind of creating a level playing field in the market.

MS. CARROLL: I think our industry feels that the FTC has a very strong culture of enforcement. But I think, look, it's a very good question to ask and it's a legitimate one and it's something we were very interested in talking about going forward. I think the question is, what does the comprehensive look like?

You know, the more detail, level of detail, there is in the law, you know, the enforcement mechanisms for that differ. But I think it's a very good question to ask.

DR. TURNER-LEE: Yeah. Karen?

MS. ZACHARIA: Yeah. It's a great question. And I'm not surprised that a lot of your members say the FTC is a really strong cop on the beat. I mean, I think

anybody who's been subject to one of those consent decrees feels that way.

You know, I was recently talking with a couple of advocates and I was surprised to hear them say that the FTC might not be the right answer. They think that some of the strongest privacy bills that we have right now and enforcement mechanisms come from a bill like the Video Privacy Protection Act and court enforcement. So I think there's a number of different ways you could go with this. I mean, I think that would be one way.

I think the FTC as it currently exists is one way in. You know, looking at additional rulemaking authority for the FTC would be a third way.

DR. TURNER-LEE: Yeah, it could be interesting. Right? I mean, some of the legislators have actually proposed bills that I think are strengthening some of the holes in like COPPA, the Children's Private Act. That was with the Do Not Track bill that's actually been out. It's bipartisan, too, a lot of the stuff that we're actually seeing.

I mean, the question becomes, you know, I've heard, Karen, to your point, well, maybe we should empower the state AGs more. Whatever federal framework that comes out, give some power to the state AGs to be able to sort be like a stronger cop on the beat on a local level because they'll be able to sort of mitigate whatever harm's there. I mean, what's you thought on the state AG role?

MS. ZACHARIA: Yeah, and, you know, there are some examples where we've done that in other things, like in COPPA, where we have a federal framework which is enforced by the FTC, but it also could be enforced by the state AG. And that's certainly something that's worth considering.

DR. TURNER-LEE: Anybody have a different opinion on that one?

MS. CARROLL: I think that's right. I think, again, it's all in the details. Right? What does the overall legislation look like and then how do you negotiate the

enforcement, both at the federal level and at the state level? But, again, I think going back to what is the end objective, right, focusing on the enforcement as making sure that we've got the user's interest at heart.

And then the second thing is that we keep this as one of the most innovative friendly places in the world. This is where Silicon Valley is, not elsewhere. And so how do we keep those objectives in mind while constructing this enforcement mechanism?

DR. TURNER-LEE: So I'm a Christian, so I don't often say the devil's in the details, but I'm going to say it now. Right? Because the details actually matter and I'm still not clear, and I think most of the people in the audience are still trying to figure out, who is going to manage these details?

Right now, the Executive Office is sort of having their own conversations on what federal privacy legislation might look like. NTIA has started this conversation. We're seeing this patchwork of bills come out. Different companies are having conversations. I mean, it was so easy on the Obama administration because it was a multi-stakeholder conversation that resulted in "Rules of the Road." But that was when the Internet was more simple.

So I'd like to ask each of you who is going to manage those devil in the details actually moving forward with this legislation and what type of process should we actually engage?

MS. CARROLL: I mean, I think those are all good approaches. Right? Again, the best outcome is when you've had a lot of use at the table from across the board. I think the outreach that NTIA and the White House has done is very useful. Again, and it's been very broad, right? It's across every sector of the economy. It's not just with a subsection.

DR. TURNER-LEE: Right.

MS. CARROLL: And it's with different nonprofits and NGOs and things like that. I think Congress also has a lot of ideas. A lot of offices are working on different bills and that's great because you get different perspectives on a range of issues. We're going to get to the best outcome through a process that involves a lot of point of views like that.

MS. ZACHARIA: Yeah, I think that's right. You know, it's interesting, I started out by saying I've been in this job for seven years. So when I started saying we should have federal privacy legislation, I'd often have after meetings a company -- like a chief privacy officer or somebody from a company would come to me outside and say, you know, what are you guys thinking? You're crazy. Or we'd go to Hill meetings in certain offices and, again, the staff would say why do you want federal privacy legislation?

There's been such a shift now and I really feel like the time is now. You know, we have CEOs blogging about why we should have privacy legislation and giving major speeches. And I think a lot of companies now think the time is now. So I do think we need input from all those places and, you know, we need to go forward and do it.

MS. O'CONNOR: This is so exciting. (Laughter) Some of us have lived a long time waiting for this summer apparently, so it's good to be in the right place at the right time. Better to be luck than smart, right?

It's all of those, yes, and, as was said earlier, you need all the views at the table, something that the process in California perhaps was short-circuited, the views of consumer groups, of NGOs, of nonprofits, of companies. We have work streams in our office of advocates, of academics, of industry, of lots of different people. And right now they're all in different rooms because they don't necessarily all agree. But, you

know, those streams will cross, to use I think a *Ghostbusters* metaphor. And I think we will think about a lot of things before we get to the right answer. But, hopefully, it will be a well-rounded and important moment for the steps forward in the use of data in the commercial space in the United States.

And some described this last year as kind of a Snowden moment for the companies, the way -- you know, I came to CDT kind of right after the summer of Snowden, and it was a very deep soul-searching time I think for government use of data. And then similarly, I think we're all thinking about what are the reasonable boundaries of self in the digital age in the commercial space?

One thing we haven't talked a lot about yet is how that plays in the rest of the world. And so I'm mindful of I have a long history of working on this and I probably won't quote all those years, but I did spend time in the federal government as a chief privacy officer and once spoke at a conference in the early 2000s of the data protection commissioners globally. And after that speech describing the U.S. framework went through interagency clearance, it was 55 minutes long. And I was nearly booed off the stage. No, not really, but I almost was. People still remember it. It was a little too long. And that's because we do have a very effective sectoral approach and we do have lots of enforcement.

When I was at Double Click we had 21 class actions, 12 attorney general investigations, and an FTC investigation in the space of 18 months. If you go look up "privacy settlements at the FTC," the Double Click letter I think is the first one still from 1999 or something like that. That's not necessarily an efficient way to run a railroad, though, right, either for a company or for the government. It also does not play well internationally.

It's very hard for consumers to understand. And as their data, again,

flows, as Melika was saying, from sector to sector, it does not provide certainty and dignity for the consumer. And it's hard for companies to comply across different sectors, as well. And what the holy grail should be, obviously, global interoperability so that individuals know that no matter where in the world their data flows, they have some sense of certainty about what the rules are that protect it, whether it's based on their country of origin or the country in which the transaction happened.

So we've got a long way to go to get there. Because the question I would have for the panel is where's that going to live?

DR. TURNER-LEE: Exactly, exactly.

MS. O'CONNOR: I don't know what the international body's going to be that's going to solve that.

DR. TURNER-LEE: Yeah. And I ask that question and, you know, we're in this wonderful place at Brookings. We're about to open it up for Q&A, so if you have questions, please start thinking about those. I see former Ambassador Danny Sepulveda.

I mean, this is a safe space, but, you know, Washington is not a safe space right now. Right? And so the question becomes can we bring -- and it's nice, I'm so happy I thought of this. I didn't really think of it until I looked at the three of you. We've got companies represented, we've got advocacy groups and, you know, a think tank. Will we be able to actually get -- you know, strike while the irons are hot or will we find ourselves where these other issues have sort of landed up in telecommunications policy where they're more dogmatic? And so, I mean, that's a question somebody can answer, but what will be the catalyst to sort of move this forward?

I think consumers have already spoken that they want something. The question will be based on the context in which we're actually living in now, if we'll be

willing to have this conversation going forward. And who will help push that forward? You can answer or you don't have to.

MS. CARROLL: I mean, I think everybody's engaged, right? And I think the question about process and whether something can get through is -- I mean, everybody in this room will have a different opinion about that. But everybody's at the table and engaged, and that's where we should be.

DR. TURNER-LEE: You think we're going to see Congress move on this at some point?

MS. CARROLL: Well, I think they already are. There are several bills that have been introduced and more that are in the works.

DR. TURNER-LEE: Karen?

MS. ZACHARIA: Yeah. I mean, it's significantly more likely now than it was two or three years ago.

DR. TURNER-LEE: Exactly.

MS. ZACHARIA: I think predicting Congress is a little bit challenging.

DR. TURNER-LEE: I was going to say, that was really (inaudible).

MS. CARROLL: Crystal ball?

DR. TURNER-LEE: Yeah, there is no crystal ball. It's called -- it's like a soccer ball, you can't see through it. You're not quite clear where it's going to land up, right? You think so?

MS. O'CONNOR: Oh, it's going to happen. I've already said in my lifetime, but, you know, we all know how old I am, so, you know, we have a runway. But somebody who is I think wise was predicting to me two to five years. It's not going to be tomorrow, but we are laying the groundwork. And yes, there are a half a dozen bills already introduced, more on the way. And I do think what you see is remarkable

alignment, alignment across sectors and alignment across advocacy and academia and industry. And when all those groups work together in some general coalition, things get done.

DR. TURNER-LEE: They do. So you heard it here first at Brookings on this platform that we will see some level of privacy legislation.

So let's open it up for questions. Who's holding the mic for us? Okay, I'm going to do this orderly. We're going to start here with a question. And if you can, narrow it down to a question so we can take as many as possible. That would be great. And if you don't have any, I've got one.

DR. ABADZI: Thank you very much. I'm Dr. Helen Abadzi at the University of Texas at Arlington. And I taught a course on the cognitive neuroscience of all this.

So the question to you is this. You're talking about data for the use, for various leaks and various intrusions. There are data that are collected in many respects are local, that is companies, like Amazon, need the data, your inconsequential data, in order to figure out how much you're willing to pay for something, such as your rent or an Amazon item. How are you going to deal with legislation given the desire to make all consumers pay as much as possible for every item, which is one piece of the question? It appears to be local.

Data are stored worldwide, that is under ice in Iceland, for example. How do you deal with that on an international basis when you started with these discussions as to which international bodies will legislate? Thanks.

DR. TURNER-LEE: Anybody?

MS. CARROLL: To the international question, international coordination's a really important question and it's a really tough discussion to have. And

on top of that, I think the conversation we're having here today is about consumer data privacy. I think a lot of foreign governments, when they want to talk with us about privacy, they want to talk about government surveillance, which complicates the discussion even more.

So I don't have any great answers for you other than recognizing, you know, the global nature of this conversation is complicated and it's made more complicated by the different interests different countries have on the topic.

MS. O'CONNOR: And just to build on that, that is an area we work on is government surveillance globally and those are very hard and kind of life-and-death questions. Right?

To your question about differential pricing, there are laws already about differential pricing in the United States. And I think it raises the meta issue of perhaps in our race to innovate and be new and fresh, we don't all necessarily realize some of the laws that apply, too, existing or courts have yet to apply existing legal frameworks to new and innovative relationships. And so I think you see that time and time again.

And I think I have great hope, actually. I may be short-term pessimistic, long-term optimistic. But the Supreme Court in this country has gotten the issues of boundaries of self and data right, I think, in large part for the last half a dozen technology cases. We filed amicus briefs in all of them. I think we've been on the winning side in five out of six, so I'm happy with that track record.

So I do think we are exploring. These are hard and difficult and issues of first impression in many cases for state legislators and for courts, but we tend to be doing it a lot of different ways and getting the right answer eventually.

DR. TURNER-LEE: Right. And I think as the technology becomes much more difficult, so some of you might have followed Microsoft's Brad Smith just came out

with this proclamation of looking at facial recognition technology and how we should legislate that. And I say those are hard -- like everybody else, those are complicated issues because you have to be really careful about infancy of the innovation with the rush to regulate or to legislate those issues.

And I think this whole idea of the information fiduciary is interesting because it goes back to duty of care. Right? When you go to a bank, you don't sign a privacy agreement that day and say make sure you watch my money. Right? You assume that there's some responsibility.

So I think your question is very pertinent, but I think we also have to keep it within the context of these emerging tech sectors.

Next question back there. We've got one right there. I'll take the man in the yellow shirt.

SPEAKER: Thank you. Do you envision preempting HIPAA medical health privacy? Can we learn anything from GMO national legislation and regulation, which hopefully will follow sometime within our lifetime?

DR. TURNER-LEE: Yeah, Karen?

MS. ZACHARIA: Yeah, I'll start with that. I think if we were starting from scratch people would probably agree that health information should be included in what we're talking about. But again, I'm very focused on trying to get to an end goal and I think that preempting HIPAA it would just make it that much harder to get to that end goal. And so I'm not suggesting that we preempt HIPAA.

DR. TURNER-LEE: Anybody else want to comment on that?

MS. O'CONNOR: I would agree and I would say there are certainly challenges of HIPAA. It seems like it's made a lot of paper and it's made a lot of disclosures, so maybe we learned from some of that and simplify. Disclosure's good in

that it forces kind of a self-awareness of the institution about what it's doing. But if it's not educating the individual about how the data's being used, then it's kind of busy work essentially.

But I agree with Karen, that's -- I'm going to just sit with Karen for a long time and get her strategy because I think she's got the right answer on a lot of this.

MS. CARROLL: And at the risk -- I'm not very familiar with HIPAA, so I may regret saying this later, but when we look at the different sectors who adopted technology to facilitate their interaction with users, I wouldn't put the healthcare industry at the top of that list. And so, again, how do we create rules that enable us to get the best out of the technology while protecting user trust?

And so if a lot of paperwork's involved, then communicating with your doctor through methods that you would like to communicate, online or whatever works for you, is not possible today because of some of those rules, maybe we should, again, modernize. How do we improve on what's there might be something to look at.

DR. TURNER-LEE: You got a follow-up?

SPEAKER: GMO.

SPEAKER: GMO?

DR. TURNER-LEE: Give us acronyms.

SPEAKER: Genetically modified organisms (off mic) federal legislation (off mic).

DR. TURNER-LEE: Oh, anybody respond to that one?

MS. O'CONNOR: Well, as a strategy, I mean, I think it would provide greater certainty to have a federal standard.

MS. ZACHARIA: Well, go ahead. Yeah.

DR. TURNER-LEE: So say that again and say it louder. Somebody

talked over it.

MS. O'CONNOR: To the extent that that raises the issue of providing greater certainty and preempting in the sense of getting ahead of a patchwork of state laws, I think there's a lot of consensus up here, I would say, about simplifying. And again, most U.S. companies and multinationals operate in least more than one state and so they would want some certainty that there's a clear standard.

DR. TURNER-LEE: Next question? Okay, we'll take this young lady in the front and then we'll go to this gentleman in the back. And thank you, these are great questions.

SPEAKER: So I work for a pretty small tech startup and I know one of the big concerns that we have at my company is that with new legislations, for example GDPR, the big companies are the ones with the means to become compliant and small- and medium-sized companies will perhaps get bought up by bigger companies or go out of business entirely or a lot of companies in my space stopped working in Europe altogether. And as we know, corporate consolidation is already a pretty huge issue in the tech industry in particular.

So how do you think we could build federal legislation that could perhaps not disadvantage small- and medium-sized businesses too much?

MS. CARROLL: So that's an important priority for us, for the Internet Association. You know, we have over 40 member companies and the bulk of them don't have offices here in Washington. Right? They're small and they're now paying attention and are very interested in this policy discussion. But that's why our goal when we look at discussing principles for legislation or when we look at legislation is, number one, how is this going to improve consumer trust? How are your users going to feel more comfortable because of this legislation?

Number two, how is it going to enable innovation with our big companies, with our small companies? But again, how do we continue to benefit from all the great tools that these companies are creating?

And finally, how is it geographically interoperable so that we don't have to create the wheel, right, in every place where we do business or where a nonprofit operates even? Right?

So those are the lenses through which we will look at all of these issues. It's really important.

DR. TURNER-LEE: Anybody else? And I would just say on that I would hope, and I've seen this with federal legislation, that depending on the size, and California did the same thing, that there are exemptions to small businesses. Because compliance could become a problem.

And you also, and I've sort of communicated this in other panels, you want to make sure any kind of national framework does not implode certain parts of the ecology just simply because data has become a natural resource of our society. So we have to just figure -- you know, I think that goes with this very cautious, deliberate, intentional conversation that needs to happen in a very collaborative way to make sure all parts of the ecosystem are actually included. So they need to be at the table, too, right, smaller businesses to ensure that they're fairly treated in the federal legislation.

SPEAKER: Thank you. My question is what should we be looking for in this Congress? The clock is ticking on the legislative calendar. Any important hearings with substantive debate coming up, markup votes? What do we look for in 2018?

DR. TURNER-LEE: Anybody? Go ahead, all three of you.

MS. ZACHARIA: So I'm not aware of any sort of markups coming up, but there is legislation that's been introduced and will continue to be introduced. There

have been some hearings. This week there was a roundtable. And I think all of that is helping to educate members.

Probably looking to the next Congress, right? Let's say that we can do the -- my hope is we can do the education now and then really hit the road running come the beginning of next year.

MS. CARROLL: I'd say of all the small pieces we've talked about or big pieces, the one that's been discussed the most is data breach. And so, you know, if -- I'm not sure that will be even likely in 2018, but that's probably the most advanced part of the discussion in all of these parts that we've had today.

DR. TURNER-LEE: Yeah, I would say I would agree on that. Okay, yeah, Deb Latham.

MS. LATHAM: My question's going to be as to whether or not we should have some bright lines that cannot be crossed. And for example, this week I was sort of shocked to read in the *Washington Post* that health insurance companies are vacuuming up data and making determinations about who they're going to insure and who they're not going to insure based upon this data.

For example, if you wear an extra-large, they think, hmm, you're obese and you probably have depression and you probably have -- and healthcare is expensive. If you live in a certain ZIP Code that's lower income you probably have bad nutrition. You may live in a home that is not well constructed and more prone to illness. And they said the health companies are now really using this type of data, and a consumer doesn't know that when you order a dress in a size XL that the insurance company has now decided that, well, maybe you shouldn't be insurable. Or even by whole ZIP Codes they're deciding that there should be higher rates in particular ZIP Codes based upon the data that they have been able to accumulate.

So I guess the question is, should there be bright lines that says no, you may not do that? And should a consumer actually have some method for determining how that data is being aggregated and being used?

MS. O'CONNOR: Can I?

DR. TURNER-LEE: Yeah, you can take that one.

MS. O'CONNOR: Yes and yes, to be very blunt. I completely agree. That's exactly the kind of research we're working on at the Center for Democracy and Technology is, again, issues of bias, implicit bias, unintended bias.

And I think actually you correctly nailed, insurance is one of the hardest areas because they're actually allowed to discriminate on some level. Right? And yet an insurance company -- we have actually done some work with several insurance companies under NDA, and one of the executive said to me we might get so good at this that we would only insure people who are insurable. And that's kind of the opposite of the point of insurance, right? Insurance is supposed to spread the risk over higher and lower level risk people.

So I think we are -- again, that's where you get to the applying old law to new technologies and saying is this -- I completely agree with you on the concept of bright lines. There are some things that are going to have to be out of bounds.

What you've also highlighted is something, and I just want to spool out this hilarious -- not at all hilarious, but hypothetical that I gave at a presentation at G.E., again, two decades ago, when we were looking at issues of home hubs and connecting your washer and dryer and your refrigerator. And I said, you know -- I actually gave a terrible scenario involving something that happened out of the home and being able to put together all the data. But the idea was imagine your refrigerator can report to the Safeway, you know, the section for milk is empty, I need more milk. Great, you know, I'm

a busy, single working mother. I want that milk on my doorstep when I get home. Terrific.

Imagine a world then when it reports to your insurance company that you've got M&Ms and white wine. (Laughter) So just saying, you know, maybe there is one day that was true.

But anyway, so, you know, it's funny, but it's not because that's the unintended secondary or tertiary use of the data in a way that is unknown, that is opaque, and unexpected to the individual. And so I do think there -- I mean, again, transparency is necessary, but not an adequate first step. And then creating the boundaries around what is in, what is out, what is simply never going to be okay. Totally agree.

DR. TURNER-LEE: Yeah. I want to just take moderator's privilege. I completely agree with that. I mean, the opacity of the data for the consumer and the inferential blocks that actually get developed because of the availability of these massive datasets are going to make these types of inferences and potential consequences very dangerous.

And for those of us that have been in this debate, we actually talked about this with the Fitbit when it first came out, whether or not your purchase of a Fitbit was a determination of whether or not your healthcare company could collect your data. And if your employer decided I'm going to give Fitbits to everybody, whoever doesn't wear it pays a higher premium, these were conversations we had like five or six years ago.

What's different now is the explosion of sensors and, as has been explained, more inferential assumptions. Michael Kearns' work on the social inferences that come from data availability, they actually lead to these consequences, which is why I think -- and again, at Brookings we're working on a paper on algorithmic bias detection

and mitigation. It goes back to this next conversation of Internet 5.8, which is how do we actually look at these things?

And, you know, Congress has taken I think a pretty cautious step around responsible use of AI. The question for us becomes what does that look like in terms of possible legislation or how is it impacted through privacy?

I think I have time for one last question and then we've got to wrap up and thank these wonderful panelists. Antonio?

And I'm sorry, if there's somebody in the back because, you know, I took off my glasses and I cannot see that far. (Laughter) If you had a burning question and I did not see you for a long time please acknowledge -- you know, let me recognize you and I can actually put two questions together.

So, Tony, ask your question. I'm going to ask this to kind of remember. And then this gentleman back here who I cannot see, have him ask his question, and then we will answer those last two as we wrap up.

SPEAKER: So I was curious about data portability. And in particular, you know, how do you measure that against privacy legislation? And when you look at companies like Amazon that both have their retail, but also own a shopping chain in Whole Foods, does that -- you know, how does that manage and, you know, what control should or shouldn't consumers have, you know, using it across businesses?

DR. TURNER-LEE: Okay, so hold that, data portability. And that young man that I could not see, I apologize. Your question.

SPEAKER: So at a separate panel I had heard that the GDPR was characterized and separated from the U.S. perspective on privacy in that with the GDPR all processing is unlawful unless it's specifically justified under one of the six bases. Whereas in the U.S., all processing was lawful unless the data fell into one of the

categories, like with HIPAA. Do you think that model in the U.S. is going to continue or that it will shift given the GDPR's influence? I know you mentioned earlier that privacy is cultural. Or will we see something where all processing is lawful, but now there needs to be increased transparency of the justification?

DR. TURNER-LEE: Okay. All right, so that's a GDPR question and data portability. So let's start with data portability and then the GDPR question as your closing statements.

MS. O'CONNOR: I'm so glad you brought up portability because we hadn't gotten to that and I think it's so important. And the other really nerdy thing I would say is data deletion. And if you saw my closet, you would laugh because I don't get rid of anything, but, you know, data deletion is a really powerful tool for companies and for individuals.

Portability. So there's a huge debate right now about antitrust and competition and how to decrease our level of the power between the individual and the institution. I think portability actually is a different set of tools that we could use to say if the individual has, again, a boundary around self and digital self and can take that and move it around, and I think you've seen is it Microsoft has come out with a big initiative in this are, that's another way to kind of level the power differential. So I'm a big fan of portability and deletion.

On the GDPR, I've heard that exact analogy with the Data Protection Directive, its predecessor, that there's a presumption of anything being out of bounds unless specifically articulated and the reverse being in the U.S. I think you're seeing actually a merging of -- not merging. I think we are all coming to the realization that data about us is very powerful in the digital world and that we all want more control, whatever country we're living in.

MS. CARROLL: Yeah, I mean, on data portability, several of our member companies actually announced an initiative amongst them this week to facilitate that. I think, again, we're all focused on user trust and user choice. And if that's what the users are demanding and expecting, I think the companies are very interested in working on that and some of them have announced that this week. And, again, we're still working on what we're hoping to see in privacy legislation. That's certainly one of the topics that we're talking about.

And then on GDPR, again, we think that we should be looking at a model for the U.S., and that enables, again, both a consumer trust, increased trust, and also the innovation that we have developed here in the U.S. And so the model that we go forward with should be focused on that versus what's happening in Brussels.

DR. TURNER-LEE: Karen?

MS. ZACHARIA: I'm going to take them in the flip order. GDPR, I think it's a little bit of an oversimplification to say that the U.S. model is everything's okay unless it's not. All companies have privacy policies. Not all, but most do. And that makes a lot of things out of bounds, right? We're telling our consumers how we're using information, what we're collecting. And if we don't follow that, then we have the FTC there to come after us and say, no, no, no, you got it wrong. So I just think it's a little bit of an oversimplification.

On the data portability, I'll say this, it's going to date myself, but Verizon was one of the first companies out of the block to support number portability. It's not quite the same, but I think exactly that. I think it's really a --

DR. TURNER-LEE: Karen, you did it yourself. (Laughter)

MS. ZACHARIA: I think it's a consumer issue. And I think that to the extent, you know, it makes sense to do it for consumers and something that consumers

want, we have to figure out a way to do it.

DR. TURNER-LEE: So on that, I think, you know, if you're looking for a facilitator for this multi-stakeholder conservation, I think I got a lot of glaring agreement on a couple of topics and I will volunteer. (Laughter)

So I want to thank our panelists. I think overall privacy legislation as we put in the title of this session, "To Legislate or Not," clearly we need to legislate. And so what we've taken from here are some cues I think of what we were looking for here at Brookings to sort of extend that work.

We're going to continue to talk about it, much like everybody here. And those of you in the audience, keep following us on that and we will get into the deeper issues of how that actually applies to AI and algorithms as that field also progresses.

So let's give them a big round of applause. (Applause) Thank you for coming out to Brookings with your time and thank you, panelists, for being here.

MS. ZACHARIA: Thank you, great to be here.

MS. CARROLL: Thank you.

MS. O'CONNOR: Thank you.

* * * * *

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