THE BROOKINGS INSTITUTION

PROTECTING INFORMATION PRIVACY: CHALLENGES AND OPPORTUNITIES IN FEDERAL LEGISLATION

Washington, D.C.
Wednesday, September 11, 2019

Opening Remarks

CAMERON KERRY
Ann R. and Andrew H. Tisch Distinguished Visiting Fellow,
The Brookings Institution

Panel 1

BENJAMIN WITTES
Senior Fellow, Governance Studies, Editor-in-Chief, Lawfare,
The Brookings Institution

SALLY GREENBERG
Executive Director, National Consumers League

DAVID HOFFMAN
Associate General Counsel and Global Privacy Officer, Intel Corporation

CAMERON KERRY
Ann R. and Andrew H. Tisch Distinguished Visiting Fellow,
The Brookings Institution

LYDIA PARNES
Partner, Privacy and Data Protection, Wilson Sonsini Goodrich and Rosati

Panel 2

MICHELLE RICHARDSON
Director, Privacy and Data Project, Center for Democracy and Technology

DYLAN GILBERT
Policy Fellow, Public Knowledge

STUART P. INGIS
Chairman, Venable, LLP

NEEMA SINGH GULIANI
Senior Legislative Counsel,
Washington Legislative Office, ACLU

BERIN SZÓKA
President and Founder, TechFreedom

DENISE ZHENG
Vice President, Technology and Innovation Policy, Business Roundtable

* * * * *

P R O C E E D I N G S

MR. KERRY: Good morning. I am Cam Kerry, a Distinguished Visiting Fellow here at the Brookings Institution. I'd like to welcome you this morning.

Before we begin, in light of the date, in light of the hour, I would ask for a moment of silence to remember those who died in 2001.

Thank you. So I want to welcome you again this morning to the Brookings Institution to the privacy debate and to this morning's doubleheader on privacy legislation. Of course Congress is back to work this week and privacy legislation has been in the works in a serious way for more than a year now, but committees are still drafting, still working toward agreement, and I don't think any of us know when we will see what may be a vehicle for legislation. But I continue to believe that the issues at stake can be resolved, and that's what we're going to explore today.

So our first panel is going to be moderated by Ben Wittes. Ben is of course well known for his work at Lawfare and his frequent news commentary. And part of the Governance Studies Program here at Brookings is down the hall from Lawfare, so we bask in their reflected glory. Ben of course has also explored what he has called the privacy paradox and some of the ways that what's seen as privacy invasive can privacy protective.

Our second panel is going to be led by Michelle Richardson who leads the

privacy work at the Center for Democracy and Technology, work that includes drafting a model privacy bill.

Ben and Michelle will introduce the rest of our excellent panelists today.

Before they do that I want to frame a little bit the issues in play. Over the past several months of focusing on the privacy debate here at Brookings, I've had a lot of discussions with a spectrum of privacy and consumer advocates in business organizations and trade associations and companies. We've had roundtables, a lot of individual conversations, public events like this, and off the record discussions. And based on these discussions, I put the issues in play into four groups based on how much agreement there is and how hard it is to reach ultimate agreement, how hard substantively, how hard politically. And in the high agreement, low complexity quadrant, we have access, correction, deletion, and portability, transparency, and notice. You know, I think almost every group that's put something out has some version of these individual rights. Details differ, but those are details that can be worked out. And I don't think anybody is going to block a bill based on those.

Then we come to a more important, more sensitive set of issues, but issues that I believe have solutions. So those include the scope of information, how we deal with the identification, and the basic principles of the FTC in charge -- not everybody agrees, but there's broad agreement on that, on a role for state AGs, on including data security, on having some accountability provisions. And I think, you know, what goes into FTC authority. The principles at least that it needs or defined legal authority, it needs more resources, it needs penalties authority, some amount of rulemaking. But, you know, all of those are things at which there's agreement at a high level, but the details matter a lot more to people than they matter a lot more to the outcomes. But I think that there's the possibility of middle ground.

Then we come to what I see as the crux of the debate, and that's what are going to be the limits or the boundaries on collection, on use, on sharing of information, and

how do we deal with the issues of algorithms and of potential algorithmic discrimination. These are big issues, they are substantively complex. In the case of algorithms we're still trying to understand some of the issues, and there are a lot of ways to come at them and they will have the biggest impact on individual privacy and potential impact on existing business practices and business models.

And that brings us to what I call the end game issues -- preemption, private right of action are issues on which there's going to be impasse unless we resolve the preceding two sets of issues, the hard issues, the solvable issues.

So these are the issues that you will hear, those sets of issues of what I think you'll hear the most about today. And I believe that if we put the panelists here today in a room for a few days that we could come up with legislation that could win broad support.

So I hope that our discussion today can help chart a path forward in that direction and the legislators can catch up to where stakeholders are.

So with that, let's turn it over to our panelists.

Thank you very much for being here. (Applause)

MR. WITTES: While all of my fellow panelists are being mic'd, just a couple of housekeeping notes. So this first panel is actually, as the program reflects, a live recording of the Lawfare podcast, and that should affect the conversation very little, but it does create two things that I want to flag for you. The first is that I'm going to introduce the panelists in the context of reading the opening script for the podcast, so it's a little bit artificial for you all as a live audience. And there's one thing you all have to do, which is that when I say I'm Benjamin Wittes and this is the Lawfare podcast, some sort of show of enthusiasm is always appreciated, if only laughter. (Laughter) The second thing is when I do this introduction, I'm going to misstate the date. And the reason is that this podcast will run on September 14, not today. So the date associated with the opening of the podcast is that date, not today, so don't correct me. I know it's September 11.

So, with that, I'm Benjamin and this is the Lawfare podcast, September 14,

2019. (Applause) We are live in Brookings' Faulk Auditorium. Congress is back, and amid all the legislative dysfunction, a consensus of sorts is emerging on the need for privacy legislation between European pressure, data preaches, and scandals associated with social media manipulation by foreign actors, the idea of some kind of comprehensive privacy legislation has gone mainstream in the last couple of years and members of Congress are hard at work on the idea. But while people agree over the idea of privacy legislation in theory, the substance of that legislation, that is, what a privacy bill would actually do, is fiercely contested. And that is what we're here to talk about, competing visions of what we're trying to do when we talk about comprehensive privacy legislation.

We have an amazing panel to discuss it all, a panel that represents a number of different competing visions of privacy legislation.

David Hoffman is the Associate General Counsel and Global Privacy Officer at Intel Corporation, and he teaches private cybersecurity and privacy policy at Duke. Sally Greenberg is Executive Director of the National Consumers League. Cam Kerry, whom you just heard from, who is not actually on the far left there, is a Distinguished visiting Fellow here at Brookings and served as General Counsel and Acting Secretary of Commerce during the prior Administration. And Lydia Parnes is a partner at Wilson Sonsini where she chairs the privacy and cybersecurity practice. She served as Director of the Bureau of Consumer Protection at the FTC.

So let's get into it. It's the Lawfare podcast episode 542, what should privacy legislation do.

So, Cam, I want to start with the point that you made in your opening presentation, where you said there were a series of issues that reflect a high degree of consensus. And I want to go back even before you get to the issues that are a consensus and just the question of how this consensus about the need for legislation in the first instance developed. A few years ago it was a pretty contested idea whether there should be a major piece of U.S. general privacy legislation. Now people seem to agree on it. How did

that come about?

MR. KERRY: So I think there have been a combination of things, and you alluded to them a little bit in the opening statement, Ben. We had this cascade of data breaches over several years, and particularly heightened by the Equifax breach, because here's a company that had a lot of impact on people's lives that, you know, a lot of people had simply never heard of and didn't have dealings with. The Snowden revelations really shined a spotlight on the amount of data that's out there. I think the question then was okay, American companies, can you be trusted to keep our data safe from the government. And then along comes Cambridge Analytica, which just metastasized things because then the question became, okay, can we trust you with our data. And that has really profoundly changed the landscape.

And in the background of this, of course, you have regulation developing elsewhere. Europe's general data protection regulation and that sort of moved the bar substantially and a lot of companies have had to comply with that. And now in the works, California Consumer Privacy Act. And that's both moving the bar and giving businesses an incentive to say, look, let's have one single set of federal rules. So, you know, the landscape has been transformed by that.

A few years ago I was going up to Capitol Hill testifying for legislation and the response I get from Republicans and from some Democrats was what do we need more government regulation for. Now, you have people submitting -- lots of people submitting bills saying we need regulation and we need -- issues that I was outlining. You have lots of business organizations for whom a lot of different kinds of regulations, the FTC rulemaking, a number of other things, would have been a redline years ago. We're saying, yeah, we need that.

MR. WITTES: Okay. So, Lydia, I'm interested in whether there is still any theoretical opposition to the idea that Congress has a major role to play here in a comprehensive sense. Is anybody making the case -- are we now only arguing about the

substance of what legislation should contain or is there still an argument at all over the merits of the idea in the first instance?

MS. PARNES: Thanks, Ben.

And I actually think Cam's opening presentation really set the state perfectly. I think there is pretty much agreement across the board that this is the time for legislation. And I would underscore a couple of the issues that he just raised. You know, the developments on the state level are pretty compelling in the United States. The idea that we could have -- we certainly will have a privacy law in California that becomes enforceable the first of the year. There are other states that are following suit and that prospect of having 10, 12, 15 state laws that apply to the collection and use of data and that may impose somewhat differing restrictions and obligations on companies I think is really overwhelming. So I think the notion of the need for federal uniform legislation is pretty clear.

I also think to the point that consumers are concerned, they are concerned about how their data is being used and potentially misused and companies, particularly consumer facing companies, they care about retaining the trust of their customers. So I am not aware of anybody who is saying that there's no basis for federal legislation.

MR. WITTES: Okay. So, David, this point that one of the objectives here is to create a uniform standard and prevent a whole lot of differing state rules from regulating the same thing is, I assume, if you're a company that has to operate in a lot of different states a lot of different jurisdictions, key to the attraction of this. How much is that the driving factor for industry?

MR. HOFFMAN: I'd say it's half of the driving factor. And it depends who in industry that you're talking with, but I would say, yes, a uniform standard is critically important. The other half though is a uniform standard that provides a high protection of privacy for individuals so that people can trust their use of technology and their participation in the digital economy and digital society. That's critical.

What you saw in California was a manifestation of people's concerns of

knowing that they might be impacted in ways and they wanted to have some way to be protected. It was great that California was able to put something in force. Unfortunately, it's not a particularly strong privacy law. It's really both based on notice and consent; it really puts the burden on the individual to have to protect themselves. I think what folks in industry are saying who are really speaking out about this, say we need a uniform standard and we need it to be a strong model on privacy that focuses on putting the obligations back on organizations that are processing data to demonstrate that they're behaving responsibly.

MR. WITTES: All right. So, Sally, at one level you must be listening to this and saying, as somebody who represents a consumer group that's been arguing for privacy legislation for a long time, you must be saying welcome, y'all, it's good to see you here. On the other hand, some of the reasons that your co-panelist are articulating for the attraction of this is not consistent with some of the objectives that you would want to accomplish I think with privacy legislation.

So is the consensus here real or is it kind of optical?

MS. GREENBERG: Well, I would say from a consumer perspective there has been a drive for the reasons that Cam identified, all of the breaches and the slicing and dicing of information and consumers' growing anxiety about what's being done with their data. We need to put some guardrails around the protections that companies are giving individual consumers when they collect their data. And right now we really have almost nothing from a federal perspective. We do have the state bills, we have California, we've got other bills that are merging in the states that I think are putting -- and, of course, the European model, the GDPR -- are putting pressure on the business community to say we better get going on something, we better put something in place and get ahead of the growing storm. And I do ask myself whether there would be a push from the business community if we didn't have these pieces of law in Europe, the EU law, and California and other states coming forward.

Having said that, I like what I heard from Lydia about -- and I like what I

heard from David -- the companies actually really do care. Just a few numbers on consumer sentiment on this, this poll is extremely high among consumers -- 74 percent of consumers said it's important for them to be in control of who gets information about them and what they do with it. And this is a bipartisan issue.

So those are some hopeful points moving forward. I will agree with Lydia, though, Cam laid things out very nicely. We have some areas of agreement, but we have some very tough areas, like private right of action and preemption issues to wrestle with.

MR. WITTES: All right. So let's wrestle with them. And let's keep going with you. If you were the person who gets to write the bill and Congress tomorrow votes on the bill, give us a high altitude sketch of what a piece of privacy legislation that you would like Congress to pass looks like.

MS. GREENBERG: Well, you know, we do have a letter that circulated among 34 consumer organizations in November of last year which highlighted all the principles that privacy and consumer organizations feel are important. Privacy protections must be strong and meaningful and comprehensive, data practices should protect civil rights, prevent unlawful discrimination, advance equal opportunity, governance at all levels. So you would have to have the Federal Trade Commission involved, you'd have to have state attorneys general involved, you'd have to preserve private rights of action for violations of whatever law is in place, and there have to be banning of certain kind of clauses that we see that are ubiquitous in consumer contracts, like forced arbitration that consumers are -- in take it or leave it contracts you're forced to sign away your rights. We don't want consumers to have to sign away their rights to have privacy protections.

So those are a list of some of the items that we think are critical in any privacy legislation. And, you know, I can flesh out some of these issues, but California, as David said, is a notice and consent, but it's got a lot of very nice protections for consumers, including knowing where your data is going and who's using it and what it's being sold for and used for.

MR. WITTES: Okay. And just to be clear, are there any circumstances in which you would be willing to tolerate preemption of state law as a part of the package? That is, you know, if federal protections are strong enough, are you willing to let industry have the idea that they're only operating under a single set of rules, or is independent state privacy regulation an important principle for you on its own terms?

MS. GREENBERG: Well, as Justice Brandeis said in his immortal words, states are the laboratories of democracy. So preemption is a hard pill to swallow for a lot of consumer organizations, although Congresswoman Jan Schakowsky has said, and she's a leader certainly in the House Commerce Committee, she has said if we get a very strong bill we could imagine a world in which preemption would be acceptable. But that has a lot of devil in the details. So we can grapple with that as well.

MR. WITTES: Cam, were you wanting to jump in?

MR. KERRY: Yeah, I did want to jump in on that because I think -- I agree with Jan Schakowsky on that and it sounds like you could get there, Sally. But the question that I had sort of coming out of what you said is aren't consumers better off assuming strong protections, you know, having one consistent set of rules that they know they're operating under, sort of pretty much regardless of who they're dealing with and where they are?

MS. GREENBERG: Well, again, it depends on the level of protections, the strength of protections, whether we've got the Federal Trade Commission's enhanced powers, enhanced funding, whether state AGs can still act on behalf of their constituents, whether we preserve a private right of action. Those are really important principles to most consumer organizations. But I agree with you, I understand the anxiety in the business community of having to comply with 50 different regimes, so let's look at what's most protective for consumers, individual consumers, and let's start there and work our way through some of these difficult issues.

MR. WITTES: All right. So, David, how much of what you just heard is like well, I can work with that, I can work with that, and how much of it is like that's not what I

mean when I talk about privacy legislation?

MR. HOFFMAN: Almost all of what you mentioned are things that we can work with and I think did work with. One thing we did at Intel, because we wanted to move beyond just frameworks and principles, we actually drafted a bill with the help of a bunch of people who are here in the room. I see Pam Dixon and Tim Speraponi, and Dan Caprio is here. A bunch of people provided us input. And we think we captured most of those protections, or all of the protections. I will say the one thing that's not in the bill is a private right of action. And I will say I couldn't figure out how to draft it appropriately and I would --

MS. GREENBERG: We can help you with that, David.

MR. HOFFMAN: I'd love to talk about that. I think it's very difficult to do that in a way because one of the goals of this has to be that we want. The use of data has the potential to help us solve some of the most important problems that we have in society. We have examples right now because people do not feel that their privacy is protected. They're holding back actually on the use of their data. We actually have the worst of both worlds. We're not properly protecting people's privacy, so we're forcing people to not make their data available in ways that actually could be really good for society.

Let me give you an example in the education sector. A lot of parents are holding back on having some of their children's performance in school being used and being able to be accessible, which could be used to personalize learning experiences, because they are appropriately concerned about what protections are going to be there for the student.

What we really need to do is we need to have a law that optimizes for both that innovative use of data by properly protecting people and making sure there's very strong enforcement mechanisms against the bad actors. It's the bad actors, particularly the data brokers, that are creating the situation that real technology companies that want to use data and technology to solve social problems can't.

MR. WITTES: All right. So but I assume you would insist on preemption as

a -- I mean could you guys function in a world in which you don't get preemption of state law?

MR. HOFFMAN: Laboratories are great unless you're the living being that's being experimented on, right? (Laughter) And so I don't see how to do this on data privacy without a uniform federal standard.

MR. WITTES: All right. So, Lydia, how much of this do you listen to and say this is broadly consistent with a privacy bill that I would support or that I think makes sense, and how much of it is, you know -- to what extent does your vision of what Congress should do differ fundamentally from any of this?

MS. PARNES: So, you know, a couple of points. I'd like to kind of start on the preemption issue because I think that that's always been kind of like the game stopper. Years ago, 12-15 years ago when I was at the Federal Trade Commission and I testified many, many times on a national data breach notification standard. Now, one would think that would be simple, have one national standard for when consumers should be notified about when their information has been unlawfully accessed. And there were issues on the margins where it was hard to come to agreement, but the biggest issue was preemption. The biggest issue. And because member of Congress and stakeholders were not able to reach agreement on that, national data breach notification was never adopted. I think it is, you know, kind of truly a travesty that that's something that we are still living with, 50+ laws that have different approaches to breach notification.

You know, so I would say on this I agree with much of what my colleagues here have said and I have some areas where I think I do disagree, and other issues that I would put on the table where I think they're kind of tricky. But I would urge that this is an area where we should not let what is perfect in each of our perspectives be the enemy of what we all agree is good. I think we need to achieve the good here. It will be a real positive.

So what would I think should privacy legislation look like? International

interoperability is important. Companies like David's are operating across the globe, but so are very small companies. And to impose the costs on them of having to comply with very different laws in the U.S. and around the world, very difficult.

A privacy law should somehow be tied to the risk of injury, of some kind of harm to consumers. I think that we would probably all agree with that. I think the devil here really is in the details. What constitutes kind of consumer harm when you're talking about a privacy injury. And I think this is particularly true since the FTC seems to be taking the position that reputational harm is adequate injury on which to kind of proceed in an action and reputational injury is certainly something that could cause injury, but it's also very subjective.

I certainly agree on many of the issues that Cam laid out, kind of individual rights, the ability to access, correct, delete personal information certainly should be part of a privacy bill. But there needs to be a lot of clarity around this. I would just note the California privacy law is incredibly confusing on this, as well as many other issues. And I think data security and data breach notification should be included.

MR. WITTES: So one question that I wanted to, before we move onto Cam's vision, ask you about specifically is that in Sally's presentation of the principles that consumer groups think are essential, there's several that she mentioned that involve some degree of data handling restriction. I don't have the principles in front of me, but they were suggestive of use restrictions. And I would think that those would be again an area where if you express it at a high enough level of altitude, almost everybody would agree, but the moment you bring it down to the sort of granular level of what aren't companies allowed to do, you get into some of those algorithmic questions that Cam was referring to in the opening presentation where, you know, you're basically potentially banning a lot of companies' business models, which may be of course the point, but is also an area where the consensus is going to break down.

And I'm curious to what extent do you think that once you get out of the

zone of transparency and uniformity in rules and notification and user control, and into the land of substantive use restrictions and collection restrictions on data, the consensus falls apart?

MR. HOFFMAN: Can I just tell you that I actually think there's more convergence on use restrictions than might be apparent. I think there's been a lot of work by the FTC over a number of years to articulate what's unreasonable, what creates risk. I think the area that is actually more difficult than use restrictions is transfer restrictions. And what the responsibilities are for the parties when you are transferring data and making it available to others. I think that's going to be much more difficult to solve.

MR. WITTES: Do you agree with that, Lydia?

MS. PARNES: So I do, and they're very related issues. I think often use restrictions are kind of on the table because to some extent transparency and choice, which I do think is fundamental, I also understand the argument about too much information. You know, consumers have a lot of information and it's difficult when you're looking at privacy policies, if you don't have a law degree or you're not trained in privacy issues, to really kind of parse this out and understand what all of it means and make decisions about how you want a particular company to be able to use your information. I certainly understand that.

I think the Commission, I think many companies have done an excellent job in terms of educating consumers and providing plain language privacy policies and plain language information. I would really, you know, encourage thinking along those lines because I do think that when you get into specific use restrictions there are -- I think the debate will very likely break down.

You know, I also think when you get into kind of fairness issues and kind of equal rights issues and nondiscrimination. I would just urge everybody to remember this is a privacy bill. We can't solve all of the problems of the world or all problems that face consumers in the marketplace in privacy legislation. And I think we need to kind of remember that.

MR. WITTES: Okay. So that's a really interesting point because for a lot of people the privacy debate merges with a series of other debates, like nondiscrimination debates. And I'm curious, Cam, how severable are they really? And do you risk entering into a situation here where if you follow Lydia's advice and you say, hey, this is a privacy bill, it's not a bill about, you know, what real estate companies are allowed to do in terms of selling people houses or, et cetera, you end up fracturing the coalition because people are actually interested in this legislation and this type of legislation for very different reasons. Is it possible to think about this in a narrow context?

MR. KERRY: I think it's possible. I think there certainly are challenges. But I do agree with Lydia's notion that we cannot in privacy legislation solve all the problems of our society. But we can ensure that data use does not contribute to those problems. And I think that's the way to focus on some solutions.

So my sort of overall vision is that we should have strong limits, clearly articulated boundaries on collection, on use, and on sharing. And I think to some extent that can affect the discrimination equation because I think some of those limits on sharing have to do with respecting the interests of the individuals the data is about. And I think that includes not using that data in ways that are just discriminatory.

So I think through some accountability provisions, sensitive uses of algorithms, doing risk assessments in advance to determine what is the risk that we will engage in some form of non-prevented and prohibited discrimination here. And then monitoring the outcomes to make sure that that happens.

But I think it's also important to this discuss how we talk about discrimination. So discrimination in some respects is what data is about, right, drawing differences. There are appropriate differences and there are some that we prohibit. So I think we can say in legislation you can't use the data for prohibited discrimination, but we should not try to sort of regulate every conceivable form of discrimination in that sort of provision.

MR. WITTES: So, Cam, before we move on, you gave this admirably neutral presentation at the beginning about the contested issues and the sort of tough decisions that people have to make. And I just want to ask you, what's the right answer? Like if you were giving the non-table setting version of that and say here's what Congress should do on each of these major contested issues, what does the privacy legislation according to Cam Kerry look like?

MR. KERRY: Well, I think alluded to that a little bit. It is strong, it is focusing on how data is handled. I think David Hoffman hit the key issue is that we need to move from a bundle of regulation that has been putting the burden on individuals to manage their own privacy and put the burden on the companies that have the superior knowledge, that are gathering the data, that have tens of thousands of engineers figuring out what you can do with that data. That's way beyond what consumers can understand.

So people want control, but I think that control needs to be put in place to some extent by law. And so that means what I talked about, limits on the collection of data so that we don't continue the system we have today where if you're not in a regulated sector, essentially anything goes. And if you can collect it, some people are tempted to go ahead and collect it. Well, gee, isn't this cool. We can figure out something to do with it and some way to monetize it.

And, similarly, use of data, how it's retained. And I agree that the key issues become in the sharing of data because, you know, right now we have an ecology of information sharing that's essentially unbounded. And things like AdTech data brokerage do have the impact of spreading information around that is enlarging our cybersecurity risk, and individual privacy risk in ways that are unforeseen and uncontrolled.

MR. WITTES: And is preemption a part of the package?

MR. KERRY: Preemption is a part of the package. I think if you have strong privacy protections in terms of the boundaries, accompanied by strong enforcement, yes, it should be preempted. I mean we are talking about the internet here fundamentally. I

mean that is quintessentially interstate. And so we should have a national standard there, but a strong national standard accompanied by strong enforcement.

But also there ought to be sort of agile and adaptive and recognize that one size fits all solutions don't work, that privacy is contextual. And so strong on the front end, strong on the enforcement, but not too prescriptive in the details. I think individual rights are necessary but not sufficient, notice is necessary but not sufficient. We do that, I think we have something that's internationally operable and that on the basis of which the U.S. can regain some international leadership in privacy

MR. WITTES: Okay. So, Sally, as I've been listening to you all talking, one of my reactions has been, wow, this just sounds like the GDPR and, you know, it's a uniform standard, it's got all kinds of strong protections, it's adaptable in its enforcement because it has all the different member states each enforcing it the way they feel like it.

And so my question is how different is what you're talking about form GDPR?

MS. GREENBERG: Well, you know, there's a lot to like with GDPR because the whole concept behind GDPR is bake data security and privacy into your practices as a proactive matter. And it applies across the board, it applies to government agencies. Any organization that touches data has an obligation to look into the technologies they use and set privacy friendly options as a default. So there's a lot to like there. No, it's not perfect.

But may I pick up on a point that Lydia made about harm?

MR. WITTES: Please.

MS. GREENBERG: Do you mind if I do that?

MR. WITTES: Please. No, no, go back.

MS. GREENBERG: If I could pivot to that?

MR. WITTES: Absolutely.

MS. GREENBERG: Because a fair point on -- you know, we know class

action lawsuits can go in a lot of different directions, but what we see today, and one of the reasons why the status quo is intolerable for consumers, is there's these massive breaches. You talked about them, Cam. And what happens when you have 500 million records taken from Marriott, or in the case of Yahoo, was it, had 2.3 billion records stolen. So what we see on our end from a consumer perspective, we have a fraud center, we have this explosion of identity theft happening because the crooks have all of our information. And who is victimized by that, the most vulnerable people in our society are defrauded out of all sorts of money and goods and it is a free for all. So current situation makes that intolerable. We need to put guard rails around that.

Secondly, we've got a situation like family tree DNA. So family tree DNA collects the DNA from their customers in a contractual situation and decides to turn over 2 million records to the FBI without checking in with their customers. That sent alarm bells around to a lot of us. That is the most private, most personal kind of information, and for a company not to understand -- you said many companies have developed very positive and easily understood privacy policies. I'd like to be in those focus groups, and I'd like to have consumers in those focus groups where we have privacy policies delivered to consumers. Because what I see is I get a note in the mail -- if I decide to open it up -- in a really skinny envelope and it says our privacy policies have changed. And sometimes when you read the fine print it's actually very alarming. You know, we can share your information with anyone that we wish or we can sell your information.

So those kinds of -- I guess what I'm saying is the status quo is driving the consumer and privacy organizations to say we need to have some rule around this. Now, as I said, GDPR, there's a lot to like about it. It's not perfect, but I think we have two very good pieces of law. We have the California law. Let's take a look at that and see what we like and find our areas of consensus and places where we disagree. Let's look at GDPR.

I had dinner yesterday with someone who is with a big company who said we're ready to adapt to the California law, we've set policies that are in keeping with the

GDPR. I know companies are very concerned. Did folks see the letter from the 51 CEOs yesterday to members of Congress? We need one preemptive national privacy policy standard. So I get that and I think there's many more areas of agreement here than I thought going in. But we've got a lot of good material to work with.

MR. WITTES: Okay. So, Lydia, I want to turn that same question to you. How does this consensus reflected here look different from GDPR? And if it's really the same, or substantially similar, why -- you know, it's not like the European Commission didn't deal with the devils in the details. And so somebody has actually thought through all of this stuff. So at the end of the day are we really just replicating the process that the European Commission went through, or are we going to come out with a substantially different set of privacy policies than the European Union has?

MS. PARNES: It's a great question. I think that when you get into kind of the weeds on the GDPR, it's different. I think one issue that just kind of jumps out at me, the GDPR in particular is very kind of document driven. And David is shaking his head yes, and I'm sure he can speak to that. But it requires companies to have documented the kind of maps of their data flows and document all of their policies and practices.

Now, that might be good corporate governance for some of it. It certainly makes sense to kind of have policies and procedures in place, but a law that is so heavily focused on, you know, having all of this documentation written, it is incredibly time consuming to do this incredibly resource intensive -- data mapping in particular can take months and months for larger companies to actually complete this effort. And, you know, I would say good thing to do, you know, great to kind of understand how your data is moving around. Maybe more important to think about, as Cam was saying, and Sally, the actual uses. And I think that that's where our debate in the U.S. is really focused, not so much on kind of having all of the back end support for what you're doing drafted in every company, but really thinking about kind of the harder issues about the guard rails and how information should be used and whether it should be shared and the extent to which it should be.

So I think there will be differences in the U.S. in terms of the debate.

MR. WITTES: All right. So I want to ask David a completely unfair question, which is if I were a cynical person --

MR. HOFFMAN: If.

MR. WITTES: If. I'm not, but --

MR. HOFFMAN: Was that the question (laughter)?

MR. WITTES: I might look at your advocacy on behalf of privacy legislation and say okay, that makes a lot of sense for Intel because Intel actually has very little skin in the data game, that you guys are fundamentally a chip maker. And so what comprehensive strong privacy regulation actually is, is regulate our competitors? And we get all the regulatory certainty, the single rule, but we actually don't do that much use with data.

And so my question is, is the premise there completely wrong and you guys actually have an extensive data collection and use system? Like what is Intel's dog in this fight?

MR. HOFFMAN: Look, privacy is good for Intel's business.

MR. WITTES: Why?

MR. HOFFMAN: Because the more people use technology in innovative ways, the more people are comfortable with their data being processed. New businesses start to feed that demand across education, healthcare, transportation, energy, and the environment. That ends up driving demand for our products when people have trust and confidence in the use of technology.

The situation that we have been right now is unacceptable for our society. We have the situation right now, if you were a victim of domestic violence, your attacker for less than $10 can find out your new name and your new address that you're trying to hide from your attacker. If you are a federal judge, people that you convicted of drug crimes, their associates can find out the names and the schools where your kids go. There are data brokers out there who have compiled lists of rape victims. This is unacceptable in our

society and it's reasonable that people in California had the reaction that they had to create a law. We need a federal law. As Lydia said, we can't let the perfect be the enemy of the good. We know that we have these unacceptable situations and we know people are holding back from providing the kind of data that could help solve some of our large social problems, that, yes, that would be good for Intel. We think it's going to be good for everybody.

MR. WITTES: All right. Before we go to audience questions, and while I'm doing this question I'm going to -- raise your hand, flag me, and I'll have a microphone come around for you for audience questions.

Cam, with all of this as backdrop, give us a sense of the current legislative landscape, right, who are the major players and when should we expect legislative drafts to arise in both houses and when should we expect committees to move them?

MR. KERRY: So I wish I knew the answer to the last part of that question, the when part. The key actors, Ben, are the commerce committees in both houses. The Senate commerce committee in particular has had a group of senior leaders that chair and ranking member leader, subcommittee leaders who have been at this in a while in a working group. They are drafting and trying to work on a bipartisan agreement. And the same process has been going on at the leadership in the House energy and commerce committee. The issues are complicated. I think the real issue here is that look, there are a lot of people in this room who have been dealing with these issues for a number of years. And I look around the room and pick out a number of people who have drafted bills and spent a lot of time talking to stakeholders about how to get there. I know David Hoffman on our panel has done that.

And so they sort of understand the issues, they understand the politics. I think a lot of people in Congress are not there yet. I think there are certainly people who have been engaged in this process for a while, but they've got to socialize with other members and other leaders, and now we have other committees, there's a Senate Banking

Committee, Senate Judiciary Committee also getting in to the act. That's sort of a reflection of sort of how -- this is a hot issue. You know, 2012, 2013 I was knocking on doors on the Hill trying to find partners to work on legislation. I couldn't find any. Now, everybody wants in on this.

MR. WITTES: All right. When I call on you, please identify yourself, state a brief question stated in the form of a question. And if you can direct it to one of the panelists, that would be great. And if you drone on I will cut you off with a shocking lack of due process. (Laughter)

Sir?

SPEAKER: Thank you. I'm Dave Rabinowitz.

For thousands of years people lived in small villages, everybody knew everybody, everybody knew everything about everybody. And until the growth of cities happened about 3-4,000 years ago, privacy was not something even possible.

I'm wondering is privacy that important or should we be concentrating on the consequences of breach of privacy? For example, a couple of decades ago if you were outed as gay, the consequences were pretty severe. Today, it's not such a big deal. Should we be concentrating on keeping information secret or should we be looking at the consequences of revealing that information because it's going to be revealed.

MR. WITTES: Okay. So it's an interesting question. Sally, make the case for the value being important at all.

MS. GREENBERG: Well, I think consumers want to know if their data are being collected and shared. It polls very high. You may not think it's important. And this (inaudible) system, perhaps it wasn't. But we are in a very different world here where consumers know their data is being gathered and used and perhaps sold to third parties in ways that they don't want and they did not agree to.

So this is a -- I think it's a real concern about having your data stolen and hacked. We've laid out a couple of egregious examples. This is a critically important issue

to consumers and they want some control over how these data are used.

So that's what we're -- and I'm encouraged by my panel members who agree, it's good for industry, it's good for companies. There are some terrible things that happen when data is too readily accessible. So I would disagree with the gentleman and say in fact we're at an era where privacy is very important to consumers and we as a consumer community feel we need to get control over it.

MR. WITTES: Ma'am?

MS. SAVAGE: Yes, Lucia Savage. So in healthcare, for about 20 years, we've had a patchwork of privacy laws and healthcare seems to be going along. There may be kind of a retarded effect on interoperability. Can you talk a little bit about why a nationwide law is so important and why businesses can't accommodate a state by state laws or preserving state laws that are already in place?

MR. HOFFMAN: I'll just add something and maybe the others -- I will say healthcare is not going along. The patchwork has not worked in the healthcare area. The idea that we've segmented off data that's subject to HIPAA versus data that is provided in other contexts that could be useful, there's so much that we could do if we had a better structure around the processing of data in the healthcare area to create better clinical results for individuals, spur better advances in healthcare research and drug development. It's to me a classic case where the patchwork has not worked and needs to be modernized.

MR. WITTES: Sir?

MR. MEDINE: David Medine, former FTC and PCLOD. A suggestion and a question.

The suggestion is on preemption. Why not sunset preemption? Twenty years ago under the Fair Credit Reporting Act preemption was put in with a sunset, and when it sunsetted a lot of consumers got a lot out of the debate at the time of sunset, including free credit reports. Why not make it -- instead of making permanent, why not have three to five years of preemption of state law and see how it works out.

And my I guess question is, isn't this time to declare consent dead? We based a lot of our models on consent. You could survey this room, everyone has a smart phone with dozens of apps. How many people in the room have ever read any of their apps privacy notices, yet their information is being collected, stored, transmitted on a minute by minute basis. Shouldn't we be 100 percent focused on use and disclosure in any new legislation?

MR. WITTES: Cam, do you want to take that?

MR. KERRY: Yeah. So I think we should be significantly over 50 percent focused on use and not on consent and disclosure. Yeah, I think by and large, that has become a fiction. And, in fact, Michelle Richardson, who is leading the second panel here today, the CDT bill that she and other drafted has no role for consent. You know, I could see perhaps a limited role for consent for certain sensitive data, certain sensitive uses, but I think it's challenging to think through, all right, what is that consent form going to look like, what's going to be the user interface.

So I think I agree with the thrust of the question, absolutely.

MR. WITTES: Lydia, can I just ask you on the preemption question -- I think this is an interesting provocative idea -- could you bridge the preemption gap by saying, you know, yes preemption, but for some limited period of time and then we have to see how it's working after that.

MS. PARNES: Right. So, David always has provocative suggestions. I think it's interesting. I also think it's challenging because I think that if we're able to -- look, if we're not able to reach any agreement on preemption, I kind of think that may be a way to kind of break through a log jam on this. I think it would be better to be able to just kind of reach agreement on it.

But, yeah, if -- I will take my own advice, don't let the perfect be the enemy of the good.

MR. WITTES: What do you think, Sally? You expressed possible

openness to preemption under some extreme set of circumstances. Could those extreme circumstances include they could only have five years of it?

MS. GREENBERG: Well, as I'm sitting here listening to the discussion, I'm getting more optimistic that we can do this because there's so many areas of agreement.

But I'm thinking about your preemption issue. I think it's very interesting, it's creative. One possible way to do that is to flint that and say okay, let's let states have a few years to pass their own bills, we'll have a federal standard, we'll have a federal bill. In that period of time if states want to come in and act and they don't think the federal bill is strong enough or they think it's too strong, let them come in. If they don't act within a year or two, then we have a federal preemption scheme.

So I think all of these ideas are very worth discussing, debating, and thinking about. And if that brakes a log jam for us, you know, either flipping it or, in the way that David described it, preemption for five years. I think we need creative ideas on the table to move this forward.

MR. WITTES: David, you had a quick point on consent.

MR. WITTES: Just really quick David, I direct you to what we did on content with the Intel bill. It's posted U.S. privacy build out, Intel.com. There's a lot of commentary from experts there. And what we did is we'd still -- it's like I love with my iPhone when it asks me to consent for sharing of location data or something. We want to encourage companies to find innovative ways like that to actually make it so that individuals can consent, while we recognize in the great bulk of situations they're not going to.

So 100 percent no, but let's figure out incentives to help have it happen.

MR. WITTES: We have time for one more question, and it' is hours.

SPEAKER: I think I'm going to piggyback on that. I am a little skeptical too when corporations ask Congress to provide some oversight and write a bill regulating their activities. That seems a little questionable to me. I would question the intent, particularly when we are hearing conversations about the idea of consent being dead, which gives the

impression that corporations believe that they should have more control over a person's information than they do and the introduction we heard that parents were not sharing data that might be helpful in the educational context because they were concerned about that information being shared. And so when you see that consumer's parents are withholding information because they are concerned about how it's going to be used, how it's going to be shared, to me that's an argument that you should have more instances where people are allowed to consent, where people are given notice about how you intend to use and disseminate their information.

And so I think that it is corporate sponsored when we say that consent is dead and people don't care about the information that apps are collecting on our phones.

MR. WITTES: All right. So I will defend David Medine against the charge of corporate sponsorship. (Laughter) However, I do think you raise a very interesting point, which is like how do you get over -- you have a sort of grand coalition that includes a big chunk of industry that's thinking about this -- how do you get over the skepticism?

I'll direct this to you, Sally, how do you get over the skepticism that industry is coming in and sort of co-opting the ideas of privacy legislation in order to basically create a good working climate for industry?

MS. GREENBERG: And I share that skepticism. So that's why you need voices like consumer organizations saying, hey, wait a second, we agree with you that we have to have guardrails and regulations on how these data are used, and consumers need to have the ability to know where their data is going. And if you're willing to give consumers that information, then we move down the road. They need to be able to delete their data, they need to know it's being sold to and to say no, I don't want my data sold, and a great sense of control, not checking off I waive my right to control my data, which industry is very famous for putting all those kinds of waivers in our agreements. Forced arbitration -- I want to have a remedy if you violated the rules that you set out for yourself and the rules that we have in these laws. If you violate them, I have the right to join with others to go and take you

to court for a class action, not be shoved into an arbitration setting that you guys control.

So industry is going to have to go the extra mile to convince us that this is something that you think is both good for you, is good for your customers, and that gives consumers the kind of control they want, at the same time giving you a uniform landscape for what the rules and regulations are, and not a patchwork of 50 different states.

MR. WITTES: We are going to leave it there. Please join me in thanking our panel. (Applause) And we're going to take a 10 minute break and then we will reconvene for the second panel.

(Recess)

MS. RICHARDSON: All right, are we ready to start. Okay, well, welcome back. Thank you very much for joining us today.

The first panel was a great way to set the scene of where things are, and some of the major structural issues that are on the table, and some of the competing interests. So, we're going to use this second panel to pick a handful of issues and go much deeper on them.

We are going to choose issues today that we understand to be, and what Cam would put in those complex boxes questions, that haven't been resolved by Congress, but we see are very important to them. And there are certainly a number of things we could have chosen from, but we are drawing from the Congressional hearings, and media reports, and our own conversations with the Hill about what would really be helpful for them in moving forward.

We are going to get beyond notice and consent; something that came up at the end of the last panel. We think this is where some of the hardest questions lie, but some of the most meaningful reforms would be.

Today we have immediately here, Dylan Gilbert, Policy Fellow at Public Knowledge; Neema Singh Guliani, Senior Legislative Counsel for the ACLU; Stu Ingis, Chair at Venable; Berin Szoka, Founder and President of TechFreedom; and Denise Zheng, Vice

President for Technology and Innovation at The Business Roundtable.

A little bit of scene setting. When we say getting beyond notice and consent, we're talking about moving from a system where you ask users to make decisions about all the different companies, and types of data, and how it should be used and when, and the changes over the time. And instead of shifting the burden back onto companies, and whether we can make rules about how they collect use and share data up-front, to lessen the burden on the user and put responsibility back where it lies or should lie.

This is going to be important because we now live in an "always on" society. We seamlessly move between accounts and websites and devices, and there are literally thousands of companies touching your data every day, and you're not able to make an informed decision about every single one of them, predict the future about how the data is going to be used, and what is coming next with it.

And that is becoming more and more high-stakes, right. Not very long ago we talked about data as something frivolous, you know. You heard people say, "Well, just don't use Facebook if you don't like it." But now we know it's being piped into systems that are making incredibly important decisions about us that we just that we just can't opt out of.

So, one of the possibilities for legislation this year is that Congress makes sort of a red-light, green light list on data uses; things that are going to be presumptively legal, and things that are presumptively prohibited.

This is something that comes up repeatedly at hearings, especially in secondary uses. So, when they collect it for one purpose but then turn around and use it, or share it, for something that is unrelated to what the user signed up for.

I wanted to actually start with Stu on this question about whether and how Congress could do a red light, green light list, and the role of secondary uses in that?

MR. INGIS: Great, well, thank you; thank you Cam for having me, and us, and thank you to Brookings. It's nice to see many old friends in the room. We've been

doing this, working on this issue for many, many years. I'll kind of start there with an answer to the question.

I'm representing, in my capacity at Venable, a coalition called Privacy for America with the goal of passing Federal privacy legislation.

And the premise for the whole exercise and coalition is that the old paradigm, or as my friend, David, referred to as consent being dead -- we call that the old paradigm, which many of us, and many people in the room, helped develop over the years, which was transparency and choice, opt-in or opt-out, self-regulation or law, but really much more choice to users. And while I don't know that I'd go as far as saying it's dead, I think saying it's alive as a solution -- it isn't.

It matters, it should exist, but we need a new paradigm beyond that, that doesn't take away choices but actually looks at the world we're living in today, which is very different from when that old paradigm was developed and evolved over a couple of decades in saying, "Look, let's start with consumers, what do consumers want," right?

Consumers want data to be used in ways that benefit them, and they don't want data to be used in ways that harm them, and they want their data to be protected. It's that simple.

I think that everybody that's ever worked on these issues could agree on that. The devil is in the details, and how do you get to that.

So, in the new paradigm what we're trying to set out is, what are those uses, what are those primary or secondary uses that are appropriate, and what are those areas that aren't; building, of course, on choice.

So, in the areas that aren't, things such as eligibility determinations, credit worthiness, insurance, healthcare treatment, education, and beyond what's covered in the FCRA, which is a complex and somewhat circular law, but that would apply restrictions. Not, you can do these things, but flat out prohibition, you can't do it. In fact, you know if you gave consumers choices, 99.9% of them would say no.

Discrimination, well yes, discrimination is already illegal, but it doesn't get the focus about data practices. There's no entity looking in detail about how data is used and derived in those ways. Committing or assisting fraud, similarly; stalking. Each of those areas has lots of details behind them, but let's take them off the table. Those should be prohibited unreasonable practices.

The flip side is there are things that should be permitted. Some of them with transparency and choice, like advertising, which I think is generally -- responsible advertising, not sensitive, but just benign, traditional advertising -- put that in the green column.

Legal process, compliance with laws, use for security, data security, for safety, for authentication, for customer assistance, recalls, legal rights, fulfillment of products and services, product research.

Now, again, at some level I think everyone in this room would say that all sounds good. Policy makers would say that all sounds pretty right in where we are now. And I think that's why we're going to get a law.

There is a lot of devil in those details though. It's, is it primary use, is it secondary use, how far down the chain -- if you have data for a particular use for security, are you then outside of all the other restrictions? Can you then discriminate using the data?

Well, the answer should be, of course not, but you've got to figure out how to map those laws in and draw the legislation.

The other thing I would put also in reasonable practice is compliance with existing laws. It may be that some of the myriad of 29 Federal privacy laws, or 200 plus State privacy laws need to be amended.

But the notion that with one full sweep you'll preempt them all, or retract and have some omnibus law, is not possible. It's not just practical, it's not politically realistic.

So, if we want to make progress, I think there's some of those tenets that have to be agreed to. I'll stop there, hopefully that gives a little bit of the parameters.

MS. RICHARDSON: Yeah, anybody else to weigh in on sort of prohibited lists. This is really difficult, right?

We've always permitted companies incredible flexibility to determine context of any interaction or any product. But are there things that are just so pervasive, or risky, or offensive, that we can say this is on the no-go list? Because that's one of the most important things we can do here, is stop this case by case process of elimination that is really just killing us.

MS. GULIANI: So, I think that one issue that, to me, is very much at the crux of the privacy debate is questions around, what can a company force you to consent to, or to waive your rights for, as a condition of using that service?

It's well and good to have these limits and to say, "Well, you can't do X, Y, or Z, unless you've affirmatively gone to the person and they've said it's okay." But if you go to the average person, you say, "Well then, you don't ever get email, you don't ever get internet service." You don't ever get, I think, services that are fundamentally required to live in today's society.

What you end up with is a regime that, I think, takes you where we are today, which is what many people I'm sure -- including people in this room -- do, which is click yes over and over and over again because they need the opportunity and they need the service.

So, I think that data minimization and talking about these limits has to be hinged onto limits to the extent to which companies can force you to consent or force you to waive those rights simply as a condition of using their good or service.

MR. GILBERT: I would take a step back and answer this on a metalevel, which is not what are the specific things that should be red lighted or green lighted, but what is the standard by which that decision should be made, because you're either going to make that decision in legislation, in which case there is a standard by which you do that. Or, you're going to write into legislation a standard by with the FTC makes that determination,

either in rulemaking or case by case.

And I think it's worth starting with the 2015 Consumer Privacy Bill of Rights' approach to that, which is a two-fold standard. One, was respect for context, and then there were specific factors laid out for that. And the other was risk to consumers.

I think that's basically right. I think that's what the existing Federal approach to privacy has been. That I take those to be a refinement of the deception and unfairness standards that have guided the Federal Trade Commission for decades. But they're more specific, and I think that's a good place for us to start.

I don't think we can have an intelligent conversation beyond the obvious red-line categories that Stu has mentioned, until we're in agreement as to in general what those standards look like.

MR. INGIS: I think we're going to be seeing a lot of this conversation going on as a sub-conversation depending on the topic with this, sort of like, rules versus standards issue when it comes to privacy.

First of all, I think that we should be embracing the fact that we're going beyond just privacy qua privacy in this discussion to things that are dealing with data abuses more at large. While that, of course, makes things more complicated, it also is getting to a lot of the harms that we really do want to address through a privacy legislation.

But what that means is we do need to think about how are we going to operationalize this? Do we have things that are just, per se, unfair, for example, within a statute? Or, do we have findings of harms that would sort of be either preamble things to guide the FTC.

One idea that my former law professor, Dennis Love, and others floated around was the idea Section 5 to prohibit abusive practices, as like a little bit of a broader. That's an interesting idea, and I've raised that because we have a lot of different ideas to how to do it.

I think that generally having just, per se, unfair practices within the

legislation is going to be the best approach and provide the most guidance. So, I think we do want to be addressing this idea of how we operationalize this in addition to figuring out which topics we want.

MS. RICHARDSON: And why don't we jump to that. We were going to talk about it eventually, about rulemaking versus legislating. I like writing as much as possible into the statue.

For clarity's sake, I'm hoping we could have something clear enough that it applies to all sorts of businesses of different sizes, and business models. But there may be areas where there needs to be a gloss, or a depth on an issue that is more appropriate for rulemaking.

So, are there some issues that are better suited for rulemaking and others that can be directly legislated at this point, and what are those, right? Because this really isn't an on or off switch, which isn't really a useful debate.

It's kind of funny, if you look at legislation from five years ago, it said things like, "Go write privacy and security rules." Right? And we're more likely to see sort of a menu of certain buckets of issues. So, what are some of these that should be subject to rulemaking, and others that we don't need that for?

MR. SZOKA: And so, I ran into Adam Conner, my fellow New Mexican, just before this panel, and he said to me, "My only question for you about legislation is red or green." Which, if you're from New Mexico it's a reference as to which Chile do you prefer (laughter), and I said well, this is Brookings, so the obvious answer is Christmas, which is a mix of red and green (laughter), right?

Now, this would be funny if you were from New Mexico, you're not, so, that's okay. But the point is, actually, it is going to be a mix because we're talking about different things.

So, sometimes there are real harms. There are things that really should be declared to be, per se, unfair, and Stu's done a pretty good first cut at what that list should

be.

But, at the same time, this is the United States of America, we have a long tradition through the first amendment of encouraging the flow of information; the collection of information, analysis, research, communication through advertising. We have actual Supreme Court case law on this that in the Supreme Court's decision in Central Hudson, is why we have the deception standard that we have today.

This doesn't come out of nowhere, this isn't my policy preferences, this is how we treat information in this country, right. And the trick here is to balance those things. And I think the way that you do that is you start from the premise that as a general matter we do not want to restrict the flow of information where people are not being deceived and where people are not being harmed.

And then the questions is, well, what are those harms. Some of them are very clear. Some of them should be written into the statue, but a lot of them are not, right. And those that are not I think we need to leave to a case by case process.

Sometimes, it might be appropriate to do it through further rulemaking, but we need to have a process by which we can distinguish those things. And I think that the 2015 approach of having those two standards, respect for context -- which is again, what do consumers understand, what is reasonable in their expectations -- and then risk to users, I think is a pretty good place to start.

And that is one example of how you can blend in the same bill, rules and standards. You have a generally operative standard, and you have in some areas, rules, which might be written in advance in the statue, or might be up to the agency to write.

One of the important differences here is ultimately what this means for remedies. Because when you come down really hard on a company and you impose huge fines, not just getting money back that was wrongfully taken from consumers, but you fine them, that's appropriate where they understand where the line was. Where they knew what the line was, and they broke it, penalize them. Where the line was unclear, and especially

where it had to be unclear because we didn't really know what the right answer was, it's not appropriate to penalize them.

They made a mistake and we should get injunctive relief if consumers were defrauded in some way, get their money back for them, but that should remain our approach to enforcement going forward. And that's the flip side of the rules versus standard distinction.

MS. ZHENG: So, I want to add onto this point. Denise Zheng here with the Business Roundtable. Business Roundtable represents CEOs of Fortune 500 companies across all sectors of the economy.

We actually just put out a letter yesterday that was referenced earlier today on the panel calling for action on privacy legislation. I'll talk about that later, but the point is that when we thought about, what's the role for the FTC, what's the role for rulemaking, how do we handle sensitive data?

I mean, we thought the right way to handle this -- and I think some of these themes were mentioned already -- is context and risk, obviously, those need to be considered, but we do think it may be appropriate for the FTC to have some rulemaking authority to determine what exactly is sensitive data, and the types of protections that are afforded to that data. But we also thought FTC needs to have a robust role in all of this.

They need to have fining authority for first offenses. They should be able to approve codes of conduct that are developed by various organizations, including industry organizations that get into deeper layers of specificity in terms of how to comply with the law, and that they should have the role of providing clarifying guidance on these like, de-identification, other things.

So, I think there needs to be a balance struck in the legislation. I think Michelle, your preference for as much being written into legislation, I appreciate that, but you can't expect Congress to anticipate every single scenario. Technology is constantly evolving. You do need to have some flexibility there, and so I think the write balance is

some narrow rulemaking authority for the FTC, additional authority in terms of fines, and the ability to clarify and provide guidance on how to comply with the law.

MS. GULIANI: I think that everybody is roughly in agreement that we're probably looking at a hybrid approach. I guess, I lean more to where you are, Michelle, in saying, "I want as much as possible in the statute." I don't want to kick these things to an FTC process because we don't know what that process will produce, and I think there's a value in having our elective representatives decide on the contours of some of what we're debating.

So, what are things that I think should be written in the statute? Remedies, I think it should be clear what the enforcement looks like, what the remedies look like, and how people, as consumers, can address situations where they feel like their rights have been violated.

Questions around data minimization: what can, and can't companies do with their data. I think that there be areas where more specificity is needed in the future. For example, if there's a carve-out for certain types of research; what does that look like, what does research even mean?

That's an area where the FTC can opine more, but the idea of you can't do acts, you can't transfer this data in these circumstances, you have to get consent in these circumstances, I think that those are things that you be very clear in the law from the outset.

One, to provide that clarity for business and consumers. But, two, because I worry that what an FTC process looks like, and if we end up with regulations that, frankly, don't protect consumers, we have to, again, revisit this conversation 4 or 5 years down the line when it becomes clear that those regulations aren't doing what consumers need.

MS. RICHARDSON: Great. Next issue, discrimination. So, not price discrimination, but the result that this sort of data processing can have on disadvantaged groups, or historically protected groups.

When we first started talking about this a year or a year and a half ago, I

think people said, “Oh, no, that’s not part of this debate.” But it has come up during every congressional hearing. It is the use cases that people are asking most about. It’s the most patently unfair.

So, it’s on the table but it’s a complex issue about what's already in law and what our next step is in addressing this. I’m going to go first to you, Neema, what are some of the use cases here that people want to address, and what are some of the options Congress could consider in moving forward?

MS. GULIANI: Sure, and let me just do some level setting at the outset. I know this came up in the last panel, and a lot of people said, “Look, well, we’re not trying to solve for discrimination in this bill.”

I can assure you nobody thinks you're going to solve discrimination in a privacy bill completely; that’s a 500-year project. But you cannot disentangle our data processes from discrimination.

A good example, algorithmic discrimination, right? Algorithmic discrimination is incredibly complex. Many people have written about this. But to act like algorithmic discrimination doesn’t pose a fundamental threat, and to act like that threat doesn’t disproportionately affect certain populations -- people of color, potentially women, people based on their sexual orientation -- I think is burying our head in the sand about what some of the data practices have resulted in from a discrimination standpoint.

So, there was an example case that the ACLU litigated and reached a settlement on, Facebook and advertising, right? And who sees ads for employment, housing, and other areas that are protected under Federal law? Not just how you maybe deliberately targeted them, but how does the algorithm -- what is the result of that algorithm in terms of denying certain individuals access to employment opportunities, or housing opportunities.

And so, I think, in thinking through the legislation, what we have to do is, one, tackle this issue of algorithmic discrimination, and what that means, and either update

or clarify in cases where our Federal law is deficient. And, two, I think we need to struggle with the fact that we have exiting discrimination laws where it hasn't been tested in the court, and even from a business standpoint, businesses may have a lack of clarity. And so, it may be worth kind of looking at our existing legal framework and augmenting it to provide that clarity.

So, I think questions, issues, and proposals that have come up have been, you know, making clear, kind of, the burden of proof that would exist in algorithmic discrimination. Making clear that algorithmic discrimination is a violation of law in cases where maybe others would argue differently.

And so, those are some of the things that I think can be incorporated into a bill with the appropriate enforcement structure, and sort of hinged on this idea of data processing and collecting data to engage in these practices.

MR. SZOKA: This came up in the last panel -- I can't remember who said this, it might have been David, but algorithmic discrimination is redundant, that's what algorithms do, they discriminate according to what they perceive differences in data to be.

So, for us to have a useful conversation about this, I think we should probably set aside the word discrimination and talk about racially disparate impact, impact that differs along the lines of protected classes, right. So, we're talking about use restrictions according to impact in the real world.

And I think when you understand it that way, it is one of the kinds of use restrictions that we're concerned about because there's a risk to a particular class of users that corresponds to a category that we have decided should be a protected class.

I understand that it's useful to use the word discrimination as a shorthand for that. I think it's conceptually confusing.

MR. INGIS: I would say probably just use the word unlawful discrimination. I don't think we're going to change discrimination law in this context, and if those laws need upgrading or changing that's probably better addressed elsewhere.

The way we've been thinking about the issue is, I think you're point of data use has become so pervasive, and you didn't mention it, but you inferred it, artificial intelligence, there are new potential bad outcomes. I think sometimes those are overdrawn, but they're certainly possible, and they're certainly in many cases, unknown.

Our sense is that that's going to get solved and evolved over a number of years by practical experience and understanding. And the way we're at least thinking about it in the concepts that we're pushing forward with the Congress is, if you have a -- we're calling for a new bureau within the FTC, there are other ways to add additional resource of emphasis, whether it's in the FTC or elsewhere.

But if you put focus, and people, and resource into looking into those issues, looking into effect, not just intent, and providing guidance to companies: here's how you should look at this, here's are things that we've seen gone wrong in other places, we think that's the best way to take the next step on it.

And I don't think, I'm not aware of, maybe you've heard it elsewhere, but I haven't heard a line of people saying, "Oh, this isn't possible," or it's something we shouldn't be worried about. It's just how do you tackle it; how do you make progress on it?

MS. GULIANI: We have to be, I think, cognizant of the challenges that are being raised in addressing this issue. So, for example, with AI, or algorithms, often as a consumer, I may not know what I see, and I don't see.

I may not know that I got an advertisement, or I was offered a credit opportunity that was higher or less advantageous because I'm a woman or a person of color. And so, I think that we have to acknowledge that there are significant challenges based on data, who controls that data, and who's making these decisions about raising claims of discrimination.

So, one of the things that people have talked about is algorithmic transparency and burden of proof, right. So, if I go to court and I say, "Look, I think X bank is actually charging me more for my loan because they've tagged me as belonging to this

protected class based on the data they processed," the response back can't be, "Well, I don't have access to that data, I don't have access to the algorithm, I don't have access to any information," so I can never bring this lawsuit. And so, I think that you have to solve for questions about transparency --

MR. INGIS: So, I think the answer could be that, I'm not sure that would necessarily be a bad outcome. In some cases, it's a good outcome. The question is, if that is really a result, are there places to go, and is this law the law to solve that, right?

There is a whole panoply, in the example you used, of financial regulators whose job is to do just that, and they do, and they do it well, having defended many companies who have been accused of that, often incorrectly.

I can tell you that the regulators are deep into that. There are remedies and private causes of action in various states that allow people to pursue that as well. But the notion that somehow you just open the court to every potential curiosity of every individual around data is not really practical.

MS. GULIANI: I just want to clarify; I'm not saying open the courts to every curiosity. What I'm saying is that in cases where discrimination is happening, and it's happening through these complex data mechanisms, what we have to have is a way for consumers to get information about that, and we have to have a way for -- what I think we all recognize as -- the intent of existing discrimination laws, for those to have affect.

And so, one of the challenges people are facing is they don't necessarily understand what mechanisms are being used. It's very difficult to parse and to sort of raise a legitimate claim of discrimination because of how the discrimination is occurring in the digital context and in these new areas.

And so, if we don't address that problem, I think that we are leaving yawning gap, and we are not addressing, I think, what consumers feel, in many cases, are legitimate problems that are inextricably tied to this question of, how should data be treated, and what should it be used for, and how to we protect against those harms.

MR. SZOKA: If I could try to distill what I think I'm hearing you both say, I agree with you. The question is, how do we identify what those goals are. And I think that on a high level there are two very different ways to do it.

One would be to make a list of things that we decide are unfair. So, rational disparate impact, right, we have a list, gender disparate impact, etc., right. A list of those characteristics, of those things that are going to be unlawful.

That, in fact, I think is consistent with that Stu was suggesting at the outset. You might differ on the margins about what should be on that list, but I think that's an approach that I would support.

What I am very concerned with is the idea of instead of doing that, or in addition to doing that, of then also, or instead, giving the FTC a blank check, which is what the abusiveness standard would do, right.

We've seen how this show goes. This is what the FTC did in the 1970s when they took the concept of unfairness, without any particular instructions from Congress, without any real limits analytically as to what it meant, and decided they were going to regulate everything in America, right. That was a disaster. It led the agency, literally, almost to its destruction.

What we ought to have is a clear set of instructions. And a standard like abusiveness, an open-ended standard like that, if it's appropriate ever, it's appropriate in very narrow circumstances, such as the CFPB, which deals with financial injuries, where we know that the injury is very clear, and quantifiable, right?

That's not true for privacy. It's not quantifiable, and it's often not clear. We need to have, A, a more specific list of the per se legal things. And, B, a standard that has more analytical substance to it.

I wasn't 100% on board with the 2015 version of those standards, risk and respect for context, but I think they're pretty good, and they certainly would put the agency on a much better path, than would an open-ended standard like abusiveness.

And just one thing to note here, I keep saying the agency, we keep talking about the Commission. In the 2015 scheme, the state AGs would have exactly the same right to enforce the law as the FTC would.

So, to the extent that your concern is you don't trust the FTC, you don't like a republican FTC, remember we're also talking about the state, being democrats in particular, or republicans during a democratic administration, being able to bring lawsuits under these Federal standards case by case.

MS. RICHARDSON: Next issue. This was one of my favorites, and we're going to go to Denise first, and this is data security. Other countries have always partnered what we would all data security and privacy together, but they have moved separately here in the United States.

Right now, we have 25 to 30 state statues on data security, and there were some press reports earlier this year that it might not make it into a privacy bill. That they were hoping to move on a time frame that would preclude them to think in detail about what data security would entail. And so, it would have to move during a different process.

BRT is one of the few trade associations, I think, that called for data security to be included in our privacy bill. So, why is it important to marry this with the rest of the privacy legislation?

MS. ZHENG: Well, I think ultimately, we want to see a privacy bill pass, but if you talk to a lot of folks, they would say you can't have data privacy without having security, right. That making the information secure, the data secure, is critical to privacy.

So, with that in mind we did put our heads together and think, well what kind of language would we be comfortable with on data security in a privacy bill.

And as someone how has spent a long time working on cyber security -- I worked on the cyber security legislation back in 2010 which would have created comprehensive cyber security regulations for industry, I also worked at DARPA at the

Defense Department -- I know that being highly prescriptive, specific about particular cyber security measures in legislation is not the way to go.

You want to give organizations flexibility to adopt the types of security measures that make sense, given the sensitivity of the data, and the risks, and the types of uses, and the context, and those sorts of things.

So, in terms of what we are comfortable with as our framework outlines, we would be supportive of reasonable safeguards for security, determined by the nature and scope of the data collected, that is should be risk-based; you know, how much risk is presented or associated with the collection, use, and sharing of that data. And obviously, consideration of the sensitivity of the data. So, for example, biometric information, or health information deserves a higher level of security than, perhaps, some other forms of information.

And then especially for smaller companies, smaller organizations, medium sized organizations, you definitely have to take into consideration feasibility and cost. When we think about reasonable safeguards for securing personal data, that's what we're thinking of.

A lot of folks also raise concerns about, what happens when that data is transferred to third parties, or service providers? That sort of data controller versus process or distinction. And we think the safeguard should follow the data to the processor.

So, there should be some sort of agreement, maybe a contractual agreement, between the controller and the processor to ensure that those safeguards follow the data beyond, as it's shared with service providers and third parties.

MR. GILBERT: We agree in some ways, disagree in others. Certainly, we think that security is a critical component. It's the foundation upon which you should be building privacy legislation because yes, you cannot have privacy without security.

We also agree that this is an area in which regulations are best suited, but we need physical administrative and technical safeguards to protect the data and that's

needs to be something that is generally across the Board.

All data are sensitive in our view. There's no distinction there, and it all should be protected in the same way. But we certainly think that if, you know, if you're looking at your florist down the street that they might not necessarily need a dedicated privacy officer, or a data protection officer.

There are, however, going to be a number of most businesses are going to need to have a robust infrastructure in place to secure their data, including running impact assessments. So, we need to have a regime that's put in place that is flexible and we also have continually developing technical standards.

This is going to be an area in which it's best suited to a flexible approach rather than just trying to take a security snapshot and put it into, bake it into legislation. So, we certainly support security as part of it.

MS. RICHARDSON: Yeah, and this is somewhere that there's really more convergence on what the best practices are than privacy for sure.

And if you look at the FTC guidance over the last decade, right, then what some of the states are doing, they really are narrowing in on the reasonableness test. Sort of, what's the half dozen controls, or outcomes, you should be able to have. And that could really sort of scale to the size of your business, or the sensitivity of the data, like you mentioned.

And it's very clear, the smalls, you really don't have a whole lot you have to do, right. If you're buying off the shelf software, you make a few good decisions, and you're probably going to be in that reasonableness sphere.

But the big companies that are much more aggressive in their data collection and use, are going to have much bigger responsibilities about having lots of professional staff, and pin testing, and data mapping, Berin?

MR. SZOKA: So, two responses. One, I'll be somewhat more pro-regulatory than the Business Roundtable in the sense that there are some things that we do

know at this point that everyone should be doing. They are things like not having your passwords be 12345. I mean, there is a list of certain things that really are no longer in that gray area.

And I think those are things where it actually would be helpful for the agency to offer guidance, that could be in form of rule, it could be something like the Green Guides.

The agency has been in the business of offering guidance to regulated enterprises for a long time, and as somebody who has followed the FTC's engagement with small businesses, in particular in the LAB MD case, I actually think that would have addressed a lot of the procedural concerns that someone like me had.

Where you just said that a small business is generally going to be fine. Well, maybe generally, but in some cases, they're not.

And that's an example of a small business being picked out as having been expected to know, before the agency ever gave any clear guidance about this. That they shouldn't have been allowing the information of peer-to-peer file sharing software on employee's computers and should have been taking specific measures to prevent that because of a particular risk.

That, really, I think, at the time was not foreseeable, and then at the end of the day, when they went to trial and they brought their expert forward, the FTC, their expert testified as to the standard security practices of Fortune 500 companies, rather than small companies. That, to me, represents a real disconnect. There's an opportunity for more guidance to be given there.

But I just have to respond that also what Dylan said, the idea that all data are the same and should be treated equally should terrify every privacy advocate in this room because that's a way of saying we're not going to take special concern with particular sensitive important data. Obviously, certain data is more sensitive and deserves special protections. Obviously, we need a regulatory regime that recognizes that and that focuses attention and incentivizes companies to focus on the things that could really harm

consumers.

MR. INGIS: So, there were three reasons, I'd been in the middle of the status security legislative debates for 15 years, and there were three -- a law should have passed at the time of the first breaches that were required to be notified after the California law went into effect.

And they ultimately didn't pass for three reasons, all which I thought at the time were wrong and continue do to, but it's worth highlighting.

One was that very issue, that all data is the same, and where the particular focal point was is that public record information should be subject to vast, expensive, security controls. The shorthand was for the phone book, although the world has evolved, but you should put significant encryption around phone book, which were being made public, right, and all of the limitations around that.

The second issue was one of liability, and it was a fight between financial institutions and retailers at a high level, and it went to who would be liable in the case of a breach, which is not, in my assessment, an area that should have been in the law, one way or the other, particularly because it was irreconcilable. Those were big players that could address that in contracts. But if you put forward specific duties of care with respect to data, that's what should have been tackled. And should be tackled now

And the third is an issue that's going to come up again, but it's preemption. And what we heard from many, from your organizations, actually, at that time, was we should let the states incubate and a thousand flowers bloom. And I understand the appeal in some scenarios for that, but there's also some shortcomings there.

And in that particular scenario where the shortcoming played out was, the law didn't pass, then you had the FTC trying to set reasonable negligence types of standards -- Lydia's nodding -- but the FTC actually didn't put forward any security guidance until after LAB MD and the reason why is because they were stuck in litigation and there weren't standards, and putting forward those standards would have hurt the case in the

litigation and their whole undercutting authority.

Whereas, if there had just been agreement on those three, frankly, very marginal things back then, you would have had much broader data security across the entire country. And I think that's a failure, frankly, of people like us to get together and come up with rational approaches.

MS. ZHENG: I want to draw a distinction as we're talking about data security, it is related but also separate from breach notification.

So, I think, Michelle, you mentioned 28 state data security laws, there are 50, over 50, breach notification laws. A lot of the issues that Stu mentioned that sort of tanked the efforts to get a national standard in place, have to do with breach notification.

I think Federal privacy legislation in this go-around, we do have the 50 state breach notification laws; there may be a way to just tackle data security without having to address the notification piece and leave the state laws in place.

MR. INGIS: Yeah, that's a good distinction and it's certainly the approach we're taking, I think almost verbatim the specific things you've outlined. It makes a lot of sense; would be great progress and I think the approach we've been looking at.

MR. GILBERT: So, Berin, just real quick to alleviate your concerns, just to be clear as well, the distinction that we're drawing here is kind of, the analog to me is the distinction on this idea of data ownership.

Public Knowledge believes that you should, as a rhetorical matter, be owning your data. You should have the ability to have control. Though we're talking about it as a legal matter, we certainly don't think that a data ownership regime is the right process.

Similarly, with regard to data, every data point that relates to you over time can become sensitive when it's in an aggregate situation. So, if we need to use sensitive versus non-sensitive as ways to operationalize things within a law, then that makes sense.

But, in terms of what we're talking about, buying your bag of Cheetos and your insurance premium goes up, data is a sort of general matter, a sensitivity to it

regardless of what kind of data we're talking about.

MS. RICHARDSON: Actually, we have on our list of topics to discuss de-identification.

MR. GILBERT: Yes.

MS. RICHARDSON: Right, so maybe let's just go ahead and jump into that. Dylan, Stu, others, this is a complicated area.

I will say, I'm surprised, this seems to be one area that I feel we are losing ground on as privacy advocates. And there's a lot of confusion about, really, what comes down to student anonymous data, and whether that should be in regulation or out. So, what's the solution?

MR. GILBERT: Well, yeah, sure, I always talk about de-identification as like the secret sauce to privacy legislation -- if you're cooking, if you've got the sauce right, things can be good, but things can go incredibly wrong with your dish if you don't do it properly.

Generally, I think -- just for a little bit of table setting -- when we have a de-I, as a goal of a de-identified data set is to take away the identifying information while preserving the utility of it. We think about that.

And with regard a pseudonymous data set, that would be replacing an artificial ID, keeping the data that is separate that could be used to re-identify with some sort of physical safeguards. Usually, they're operationalized within legislation by providing exemptions often to the actual rules of the legislation.

So, for example, within the GDPR, where if data anonymized in a way that the data subject can't be identified, then processing on that data can be done free of the obligations under the law.

So, in some ways that's powerful and good, because we need to be incentivizing privacy protective data processing, as David, I believe was the one that mentioned in the last panel.

We do need to giving attention to the myriad harms that can transpire because of data processing, but data processing brings a host of public benefits that benefit the public interest, whether that's scientific, public health advancement, education, all kinds of good ways.

So, what's the problem then? Well, there are a couple of problems. One of them is with standards. There's no real universal standard around de-identification in the U.S.

In HIPAA, with our sector specific health law, there's a fairly robust regime around the de-identification that's been done through rulemaking, which I'll get back to in a second, but outside of the health context, it's a bit of a Wild West of ad hoc standards when we're talking about what de-identification means.

The second problem is de-identification is hard and it often isn't done properly. The National Institute for Standards and Technology, NIST, noticed this much when government data set were not being de-identified properly, so they issued an unlinkable data challenge to allow various organizations, and data scientists to compete on properly de-identifying those data sets so that the benefits can come from analyzing it.

Certain data are more difficult to de-identify than others. I think particularly of location data. There was one study that was done where 95% of those involved were able be reidentified using just four data points.

We also had recent EU data scientists published in nature, that I'm sure that many have seen here, that found that heavily sampled and de-identified data sets are unlikely to satisfy GDPR.

So, what the problem can be here then is, if it is somewhat easy to reidentify a data set, and you have significant exceptions baked into a law to get out of your obligations, then we have, potentially, a free pass to get out of things.

So, what do we need to do? Well, we need to make sure that the definitions of de-identification are crafted properly that compels companies to not reidentify their data.

We also need to be setting standards and provide a flexible definition of what it means to adapt to developing technology.

So, for these reasons we think de-identification is a good example of something that is best handled through rulemaking in a similar way to data security.

But we need to be incentivizing to the greatest extent possible the use of de-identification, but we need to make sure that we understand that it has a lot of limitations.

So, for example, to answer your question about pseudonymous data, if we write the bill to say that pseudonymous data is no longer covered data; well, if that pseudonymous data isn't really pseudonymous because it can be re-identified, then that's problematic.

MR. INGIS: A riddle, it is a riddle, pseudonymous data. The one thing, I agree with everything you said, I think the one thing I would just offer as an observation and maybe a way we should be thinking about this issue a little bit differently is thinking about pseudonymous data in terms of a privacy regime, and pseudonymous data in terms of a data security regime.

If you think about it in a privacy regime, and you think about it in an area of setting normative standards of people that follow law and with enforcement, you can readily come up with standards that are agreeable, and workable, and functional.

The challenge is, on the data security side, because the fear that's always raised is, "Well, somebody could hack this." And the answer is, probably can.

But if you think about them differently; if you say, look -- if you pseudonymize data and you have these contractual restrictions, other ways of taking on liability for re-matching it downstream, you handle the privacy issue as a legal matter, straightforward.

The data security thing, I think, is where you would push on what are the standards, how do you drill down, you know, what levels of pseudonymization --

pseudonymization for click streaming advertising data probably very different from pseudonymization for HIPAA related data.

But I think what happens in this debate is they get conflated. And so, I offer that as a suggestion to think it through.

MS. RICHARDSON: Okay, we're going to go to questions in five minutes. So, if you have any, start thinking about how you want to share those with us. I've got two final questions for the panelists.

Private right of action, this is another area which presents an off or on switch, but that's not how they work in the real world. Right now, all 50 state adapts have a private right of action.

They vary greatly, some have very strict harm standards, some prohibit class actions, some prohibit penalties, and other require a public interest standard. They basically have been cobbled together to really try to balance the interests of having litigation advance (inaudible) rights but try to tease out some of the more nuisance litigation.

So, Neema, your organization has been doing impact litigation for a century. What are some of the most important things in a private right of action that Congress should include if they're going to draft one for this privacy bill?

MS. GULIANI: I think off the bat, in the privacy arena, one of the difficulties and challenges people often face is proving harm, right. Think of the Equifax breach. I think we broadly recognize that lots of people's data was disclosed and that there's a harm there.

As an individual, it's very difficult to point to harms and often prove because harm is difficult in the privacy context.

So, I think that having a private right of action attached to a violation of the law, and not requiring an additional step for a consumer to then do all of this investigation to try to sort of attach different affects and harms associated with that is important.

I think the second thing is one thing people have talked about is sort of a

requirement that someone first go to the company and say stop doing this or stop doing that, before they can have a private right of action. That could be extremely difficult in a class action context, and I don't think we want to foreclose class actions.

We don't want a situation where a company is engaging in a harm, it affects large numbers of people, and now to have viable litigation, 1 million people have to send the same exact letter to a company to notify them of a problem.

And so, those are, I think, two things at the outset, but I think looking big picture, historically one of the reasons the class actions have been so important is because often the government either doesn't have the resources or will to enforce the law. And two, it's important that the individuals who are affected have a way of enforcing their rights.

And so, I see it as absolutely critical and as part of the enforcement infrastructure. And if you don't have strong enforcement, I think we risk a privacy law that is words on paper that people don't have a way to enforce.

MS. RICHARDSON: Any other thoughts of what would go in or stay out of a private right of action.

MR. GILBERT: Understanding that as the Obama Administration proposed in 2015, the state AGs would have full rights to enforce the Federal law, I really fail to see why there would a failure of will to enforce the law.

MS. GULIANI: At a practical level, the idea that you would have enough resources to enforce a privacy law, I think, doesn't reflect the reality.

So, for example, the number of people at the FTC who do enforcement, is roughly the size of the Irish DPA. Even well-resourced AGs have the number of people who focus on privacy could probably fit on one hand.

And so, you're not simply -- just purely looking from a resource standpoint, you're not going to have the resources to enforce privacy law in every circumstance where individuals are affected.

But even beyond that, even if I lived in the world you live in where there's enough resources, I think that it's important that people be able to enforce their own rights, because historically, the government hasn't always stepped in to enforce people's rights.

That's why in the discrimination context, and many other contexts, a private right of action has been absolutely critical.

MR. SZOKA: If a cost of a private right of action is dispensing with the evidentiary requirements that actually keep us grounded in focusing on consumer injury, the answer to me is very clear: fund the enforcement by government agencies that are responsible for making decisions in an appropriate policy way instead of, to be frank, chasing a payoff for plaintiff's attorneys, right.

I am all in favor -- if you want to talk about doubling the size of the enforcement arm of the FTC to do this, fine, let's have a conversation about what we need to enforce the law adequately.

But saying, for example, that the team is the size of the Irish DPA is, as you know, is quite misleading, because the Irish DPA, of course, essentially handles these issues for all of Europe because that's where these European companies are based.

So, we can have an honest conversation about what the right staffing level is at the FTC, but that's not a fair comparison.

MR. GILBERT: Well, there's a lot of talk -- look, Public Knowledge is very sympathetic to the problem sometimes of statutory damages, particularly within the copyright context, and that's a topic that's worthy of conversation debate. But we also need to remember that injunctive relief is something that is provided through a private right of action as well, which is equally important to be able to stop bad actors.

MR. SZOKA: But the government can do that too. That's why we have the Federal Trade Commission and the state baby FTC acts.

MR. GILBERT: Right, but are they always going to be acting, no.

MR. SZOKA: They're quite aggressive. They have obvious political

incentives, especially the AGs to do so. And again, if we're having a conversation about that question, let's talk about what resources they would need and how we can help state AGs coordinate.

MR. INGIS: I'll just offer as an observation, you know, put it aside, I think there are reasonable policy debates to be had here. And, I think you've heard them. And there are excesses, which is, I think, what Berin is highlighting, and they're real, they are not speculative, and they happen all day long.

As a pure political reality, I think that there is a zero percent change, in fact, maybe negative 3,000, that there will be a private right of action in the Federal privacy law.

And so, people can debate that and disagree with me, but I think that the practicality is that the public would be much better served with a uniform standard, with strong protections and then push and think about where, is enforcement strong enough, try lots of additional resources, use the state AGs as additional places to further enforce those rights. That's certainly important and I've seen in most of the proposals.

MS. RICHARDSON: Right, okay. Well --

MS. GULIANI: I know we're going to questions -- I think I might be basically; we have to agree to disagree. But I think, hopeful, again to some of those disagreements.

MS. RICHARDSON: I will just point out that this is pretty much like everything else that goes into a privacy law. There are a million choices that could be made to scope it and there is nothing inherent about a private right of action that results in massive attorneys' fees, or damages or anything else like that.

So, final question, and then hands up if you have a question. We have someone up here in the front. I will close out with you, Denise.

Timing, there is a little bit of a debate about whether we need to do this now. If there's a benefit to doing this sooner rather than later. Tell us about what we all get out of doing this over the next six months to a year.

MS. ZHENG: A lot of people say that industry just wants to see a privacy law to gut the California law before it goes into effect. I'm just going to take that on right off the bat. It's not true.

It's not about California. It's about the fact that you have different inconsistent laws across the states, and it's going to be a nightmare for consumers in terms of the types of privacy protections that they expect, the user experience for them, and it's going to impossible for companies to also comply with all these different laws, and make sure that their compliance regimes are specific to each state. It's just not possible.

And so, are we going to get a privacy law passed before California goes into effect? I would say probably no. But, can we can a privacy law passed in the next year and a half? I think we can.

So, let's all sort of work together toward that common goal, and have a robust debate about what the privacy law should say.

I think that's kind of how we're looking at it. It's complex, it's highly technical, there's a steep learning curve, there are a lot of issues to be debated. So, we should get that started now. Let's see some language, let's have that conversation because this isn't going to happen overnight.

The urgency around this is to get sort of the ball rolling, right. Let's take some incremental steps toward getting legislation passed. I think realistically, it's hard to see anything really happening in terms of final passage this year. And I don't know if others disagree with me.

MR. INGIS: Yeah, I agree with that and I think the time is now. I think that there is actually, when you get outside of some of the procedural things -- not that they're not important, like a private cause of action -- but I think substantively, there really is not very much disagreement, if any, among a broad set of stakeholders on all ways you look at it. And I think a law could be passed now with what we know. This is not a new debate; it's

been going on for 20 years plus, and it's just tightened.

And I think, you know, a comment that was raised earlier, you could put a sunset on the law, you could pass something and sunset it in five years to see whether it's working, to see whether enforcements is sufficient, and then go beyond that.

MR. GILBERT: We certainly would like to see a path forward, agree that language is everything, no one really knows what's in there right now.

So, hopefully, we can start seeing discussion drafts, whether they're partisan or bipartisan, anything. Something needs to come out so that we can all engage and start figuring out whether there is a path forward in the short-term.

But certainly, if it's looking more like the let's get CCPA, then let's do a good privacy law, then advocates are certainly not going to be interested in pushing something through quickly, but I think the time is now. We certainly agree that we should be putting all our efforts towards getting something meaningful passed.

MS. RICHARDSON: Great, the audience.

MS. TRUJILLO: Yes, thank you for a lively. It truly has been thought-provoking. So, my name is Maria Trujillo, I'm from Georgetown University.

The privacy debate is catching up to the innovation created by technology, and both panels have talked about the present, but none have issued any ideas about the future. And in rulemaking, and case by case, what's going to happen in 3, 5, 10 years, when you can't imagine what the future brings. What's the mechanism to changing these laws?

MS. GULIANI: So, for the ACLU, one of the reasons we've been really concerned about Federal preemption is for that reason. You innovate, new types of data being collected or used, you have a Federal law that essentially, depending on how your preemption is drafted, could tie states from them passing laws that would protect that.

So, one of the reasons. I think we've urged preemption to only really cover, let's say, a situation where it would be impossible for you to comply with state and Federal law. You're really frustrating the Federal law itself, but then leave states free to kind of, I

think, those renovations and challenges.

MS. RICHARDSON: I think one solution that we've endorsed is trying to regulate types of data uses, or types of data, right. We probably don't even know what biometrics are going to look like in 10 years, but they're still going to be biometrics, right. Or location will be location, whether it's an implant, or your phone, or your car.

So, one way is to try to define those regulations in those terms because they'll be flexible over time.

MR. SZOKA: I think that's a great question, it's the same question the FTC grappled with, it's what the Unfairness Policy statement is all about. You should reread it, there's a great paragraph in there on exactly that topic.

My answer is, the kinds of harm we're concerned about, those are the things we understand. They are relatively static; those can easily be fixed in legislation.

We don't know what the fact patterns are going to look like and that's why I, as a general matter, think we should prescribe specific harms, deal with the specific things that we know are problematic today. And then have standards that are capable of addressing those problems, while also not allowing the agency to go too far. Or, even worse, creating a cloud of uncertainty that chill people form doing things from doing things like research.

We haven't talked about health data. To the extent we're talking about health data in all this discussion, the stakes here are literally life and death. If the cloud of uncertainty around legislation prevents people from doing research, real people will die, and we will not see those losses, probably.

Just as happened with Viox. Viox was on the market for years longer than it should have been because existing privacy law made it difficult to diagnose that it was Viox that was killing something like 50,000 people a year. These are the stakes of what we're talking about.

MS. RICHARDSON: Back of the room.

MR. COCHETTI: My name is Roger Cochetti, and I'm one of those pioneers Stuart was referring to in the opening. Nice to see you again, Stuart, and I'd like to ask a question which is sort of a broader, pulled back a little bit, and look at the bigger picture.

And, by the way, for those interested in the bigger picture, I have an op-ed in the current hill which covers the four major blunders we made in the 1990s when we created the legal structure for the internet that exists today.

But my question is, really, if you take many steps back, does it really make sense to try to isolate the subject of privacy from all of the other emerging internet issues, and statutorily, or even regulatorily, try to deal with the privacy topic by itself.

And I illustrate the reasoning behind my question to say, if you were to ask any high school student today, "Should we treat the internet more like postal mail, television, telephone, or newspapers?" Their answer would be instant, "What's postal mail, what's telephone, what's television."

You know, inevitably, the sectoral approach pulls regulation into different characterizations of the medium in different directions and we wind up risking a different view of platforms, a different view of national security, a different view of cybercrime, a different view of free speech, if we take these topics one by one.

And I'm not sure I know the answer to it, but I was interested if any panelists has any idea whether the time is ripe for not sectoral updating, but rather comprehensive updating because of the fact that these are interrelated and if we take them sector by sector, we have a risk of having an uncoordinated approach to the medium in the future, thank you.

MS. RICHARDSON: I mean, my understanding is that it's not going to be sectorial privacy, it is going to be anybody who holds personal information. Maybe they leave banking or health intact under the current statutes, but I think people do not want to marry the privacy and security debate with --

MR. SZOKA: Net neutrality --

MS. RICHARDSON: Net neutrality, content moderation, elections security, sort of the whole universe of internet issues that have come up over the last year or two, because getting a privacy bill is going to be so complex, adding in all those over equity is just going to make it immovable.

MR. SZOKA: Yeah, I mean, certainly the tech policy issues are going to be very interrelated and it's good to be thinking about not redoing privacy policy in a vacuum without thinking about competition, without thinking about other implications. But, agree, that we should be focusing on privacy as a legislative matter.

The question is, is politically, are some of these other committees looking to get in the game and then suddenly we have an omnibus approach and it really drags out, so that's an open question, I think.

MR. INGUS: I think you could maybe try and distinguish a little bit between -- it won't be perfect, but -- types of entities versus types of data, and I think in the examples you used, Roger, on the different types of platforms, that, to me, is more in the types of data categories, and maybe you can break down some of these other statutes that are treating the same, whether it's the Cable Act, or the Video Privacy Act, differently.

I think it gets harder both substantively and politically when you start talking about health data, or financial data, the types of data.

MS. RICHARDSON: Any final questions from the audience? Okay, the last three minutes. How about everybody go down the line and say the number one thing you would like to see in a privacy bill this year. Three sentences, this is a surprise question.

MS. ZHENG: We just want to see one consistent Federal standard.

MS. RICHARDSON: Okay.

MR. GILBERT: The most important thing is to get the identification right. I disagree with most of what Dylan said because he's focused on people screwing up the identification. Of course, the point of the 2015 bill was that there would be, it's not a free

pass, there are standards for that and there are lots of ways that you could address concerns about abuse.

Joe Gerome made an excellent suggestion; if we're concerned about how people will be identifying data, maybe they should have to disclose to the Federal Trade Commission what their identification practices are.

There are ways of dealing with these concerns, that don't throw the baby out with the bath water because de-identifying data is the way that we're going to do most of the valuable research into data analysis.

You get that wrong, and we've started at the wrong place from the outset. We're imposing much larger costs on research than we need to.

MR. INGIS: For the first time in a long time there's an almost ubiquitous consensus among the business community that a law would be beneficial, and I think it creates an opportunity. And I think the unique part of the opportunity is that none of the proposals are pushing for like a CCPA Federal version. It's really a much more detailed scenario.

MS. GULIANI: I would say preserving states ability to put in place higher standards. I guess I'll cheat and say to a private right of action.

MR. SZOKA: I like to see strong enforcement at the agency and state level, including individual level private right of action.

MS. RICHARDSON: All right. Do you have anything to wrap us up with, Cam?

MR. KERRY: Sure. Thank you very much. So, thank you to Denise Zheng, Berin Szoka, Stu Ingis, Neema Singh Guliani, Dylan Gilbert, and our moderator Michelle Richardson (applause).

I just want to note, male fashion comment that the Twittersphere has selected Stu Ingis as the winner of the sock game (laughter).

So, thank you all for coming. I do also want to thank Intel Corporation for its

support of the Brookings institution. We encourage broad based support. We do have individual memberships, and other institutions can participate, but that does not influence the opinions of any of our panelists, or our work at Brookings. We look forward to continuing the privacy debate through a variety of forums.

As I said at the outset, if we put our panelists here today together, we could get to legislation. We haven't quite gotten there, but I think, perhaps, that we have helped to show a path forward. So, thank you all for helping to do that (applause).

* * * * *

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