FINISHED FILE

INTERNET GOVERNANCE FORUM USA 2021

The Future of Data: Privacy Foundations and Legislative Approaches

JULY 15, 2021

1:30 P.M. - 2:45 P.M. EASTERN

Services Provided By:

Caption First, Inc.

P.O. Box 3066

Monument, CO 80132

1 877 825 5234

+001 719 481 9835

Www.captionfirst.com

***

This text, document, or file is based on live transcription. Communication Access Realtime Translation (CART), captioning, and/or live transcription are provided in order to facilitate communication accessibility and may not be a totally verbatim record of the proceedings. This text, document, or file is not to be distributed or used in any way that may violate copyright law.

***

>> DUSTIN LOUP: Welcome, everybody back from the break for this session on the future of data, privacy foundations and legislative approaches. I'm going to hand it over to Stu Ingis, Chair of Venable, to moderate this session.

>> STU INGIS: Thank you very much, Dustin, and it's good to be with all of you. I got great privilege of moderating a very distinguished panel. I will briefly tell you who they

are, but then I will let them tell you more about themselves and their perspectives and then we will engage in a good back and forth among the group.

So in the order that I have open my list, I will say to Marty who I have probably known the longest of all the folks here, we will put the least important first, after me. Marty Abrams, the executive director of the Information Accountability Foundation. Jennifer Huddleston, the director of technology and innovation policy, at the American Action Forum. Peter Winn, the acting chief privacy and civil liberties office for the US Department of Justice, and Jane Bambauer, professor of law at the University of Arizona. And the reporter for the uniform law commission, which is very engaged in this issue right now.

So welcome to all of you. Why don't we dive in, Marty, tell us what you're doing these days on privacy and give us just a little bit of an intro.

>> MARTY ABRAMS: So I'm Marty Abrams, I have been doing privacy for over 30 years now. And have been doing that privacy work globally. I run The Information Accountability Foundation which was the incorporation of the global accountable dialogue which defined the concept of accountability that's being built into many national laws, and we look at the question of how organizations can have the freedom and the flexibility to use data wisely, while at the same time protecting individuals from -- from negative outcomes from both the processing and the not processing of data.

>> STU INGIS: Great. Thank you, Marty, and welcome. Jennifer?

>> JENNIFER HUDDLESTON: Thanks for having me. My name is Jennifer Huddleston and I'm the director of technology and innovation policy at the American Action Forum, broadly speaking my work covers the intersection of law and technology which of course includes the issue of data privacy, and I have written a lot about the different ways that state laws may be

impacting the overall approach to the data privacy and how that could impact discussions around federal policy, as well as the tradeoffs involved in the data privacy debate when it comes to issues such as innovation and speech.

>> STU INGIS: Great. Well thank you and welcome to you.

Peter, nice to see you. Tell us what you are up to these days.

>> PETER WINN: Well, as you mentioned, I'm the acting chief privacy officer at Justice Department, and by way of background, the Justice Department includes most of the federal law enforcement agencies, including the FBI, the DEA, alcohol, tobacco, firearms, marshals and so forth, all the prosecutors, folks representing the government, immigration judges, just a whole host -- about 150,000 people if you include our contractors.

So my job is to basically make sure that everybody -- I have two functions, one is policy, I advise on new ideas about privacy, but I -- and by the way when it comes to affecting people's data, that's pretty much everything we do at the Justice Department. But I also have the responsibility to make sure that the 150,000 employees and contractors that we have do what we say they are supposed to do, do what the law requires them to do and that's a compliance responsibility.

And ultimately -- ultimately, privacy is about trust, and if you -- if we, for instance, the Department of Justice or a business, but if we don't do what we're retired to do under the -- we are required to do under the law, then we will lose the ability to get the information that we need to keep people safe and protect national security. So ultimately, trust is mission critical and that's true not only for the Department of Justice. It's true for businesses that have to maintain the trust of their customers.

And so what I have been doing on my policy side of the house, is really trying to work to help figure out of the best way to have laws that results in people doing what they are

supposed to do, so that we can maintain trust in the data that is -- is essential social resource that we all use and need to be both either efficient and protect the privacy data.

>> STU INGIS: Well, thank you for that introduce, and finally, most important since we started with east as I was saying, Jane, thanks for your patience. Tell us a little bit about yourself and your work -- your dual roles, actually.

>> JANE BAMBAUER: Yeah. Yes, I'm a law professor of Arizona, and I got involved in privacy from a strange angle. It's how I see the policy development. I started off seeing the unintended negative effects of otherwise well-intentioned privacy laws on -- in terms of how it affected research and public accountability, things like FOIAs, privacy exception and so I started sort of narrowly trying to figure out in my research and some of my pro bono work, trying to figure out how to best mitigate the tension between the control over new knowledge that privacy embodies, versus the liberty to create new knowledge and to use it, that -- that free speech and other -- and other public values embody.

And then more recently -- I started to narrow in on thinking about research, the impact of privacy laws on research. At this point, I'm writing pretty actively about pretty much all areas of big data and privacy. And as you mentioned I'm also serving as reporter for the Uniform Law Commission, which just got approved at the annual meeting, and that tries to draft a -- an alternative to the sorts of legal proposals or enactments that we have seen in California and Virginia.

>> STU INGIS: Great. Well, thank you, and congratulations on that -- that thoughtful input to the whole dialogue. And hopefully we'll get into a bunch of issues here. So let's start out by really diving in, you know, we'll ultimately wind up with concrete predictions and what bills and laws may happen. Let's start off at the highest level. Peter started us already a little bit into, it but just what is privacy? You

know, it's such a broad topic. Jane, you are writing about it in -- never a shortage of things. And Marty is on his fourth decade of writing about it.

Why don't -- Jane, maybe you can go first here, and just what is privacy? How should we be thinking about what we are solving here?

>> JANE BAMBAUER: Yeah. So it is quite an abstract concept and one the things with privacy discourse, it has the quality to be whatever people want it to be and sometimes we wind up talking past each other or not recognizing the tradeoffs that have to be made. But I would say at a high level, we want to recognize in legal form or norms, if necessary, some amount of control that people have in terms of their seclusion or the secrecy that they can expect, or the downstream uses of information about them, that describes them and that is about them.

So that's why I described it as a constraint on knowledge, and I know that kind of puts it negatively, but it is useful to constrain what people do with information in a lot of contexts but the other reason I like that framing is that you can see the downsides too, that -- that usually and historically, at least as far as courts have -- for the most parts courts have interpreted American privacy, the default has landed on the other side, that in general people have liberty to use information in novel and creative ways, unless there's some recognizable threat to some minimum level of seclusion or some downstream harm that is predictable and, you know, not -- not too speculative.

So that's how I would encapsulate it.

>> STU INGIS: Marty? Thank you.

>> MARTY ABRAMS: When I think about privacy, the term privacy is used in the United States and much of the world it really encompasses three interests. First is the interest of a space where I'm not viewed. I'm not seen. A place where in my house, unobserved by others. The second is the ability to

control the knowledge about me, you know, be able to define myself and not be defined by the body of information that flows around me.

And the third and increasingly most important in an observational world is that the data is used in a fair fashion. That data is used in a fashion that is -- that if it's harmful, it's harmful in a lawful way and not in a capricious way. It's interesting in the United States that the first privacy law enacted was the Fair Credit Reporting Act which is a fair processing piece of legislation that begins to describe with the fairly abundant information collected for credit reporting that it be only used for permissible purpose and that's a fair processing piece of law.

In European law, as you know, Stu, we split the concept of privacy as a matter of seclusion and that's under a fundamental right to family life and the other is the fundamental right to data protection which encompasses all the areas that are impacted by the -- by personal data.

>> STU INGIS: Great. Thank you, Marty. Jennifer, let's bring you back into the discussion.

>> JENNIFER HUDDLESTON: Yes, I was going to jump in and kind of pick up on what Marty and Jane have already said. I think at least colloquially, it's incredibly important to talk about what we are not talking about when we talk about data privacy. Oftentimes in the policy framework we hear concerns about data breaches or data security issues which are very important issues in data protection but should be distinguished from the data privacy conversation, from things like what Jane and her colleagues are working on at the uniform law commission.

I also think it's important to distinguish between data privacy and consumer privacy context, issues where we are talking about the consumer relationship, to a company that may be collecting data or what sort of rights we perceive in those fashions, and kind of the privacy and the freedom from

government surveillance sense, the concerns about what the -- what information the government may or may not have access to, questions of fourth amendment rights. Those are also privacy questions of a certain sort, but they are handled very differently and the way many of us would view them are very different than how we view this traditional consumer privacy question.

>> STU INGIS: Right. And thanks for distinguishing that.

On the focus which is I think going to be our primary focus today on the consumer privacy angle, Peter, tell us anything else you want to aced to what you had said earlier about generally what privacy is, but then maybe you could start us off on how do we start thinking about taking these broad concepts of rights and philosophy tied to them, and boiling it down into stuff that's meaningful and actionable, both to consumers as we just discussed and understandable by businesses.

>> PETER WINN: Thanks, Stu. I since I'm from the government, I wanted to highlight what Jennifer just said. In the United States we have strong privacy protections again the government, reflected both in constitution and in our statutes like the privacy act.

And you know, people are in control of their government. There has to be some limit to the government's ability to control them. And so that's why we think people ought to will have the right to be left alone. Freedom of thought requires privacy of thought and that's a precondition of civil society and democracy. You know, everybody knows authoritarian states don't respect privacy. We forget the crucial role privacy rights and keeping democratic governments from becoming authoritarian.

The difference, however, in the United States, privacy we think of as a fundamental right, but we believe it's about protecting mutual trust between government and the people in connection with the democratic society.

You know, the commercial sector, Americans don't typically consider data protection to be a fundamental human right, but a means to promote mutual trust, between individuals and organizations, and so that's really as you said, Stu, what we need to be focused on. And here there's a tremendous amount of confusion and misunderstanding that -- that Jane and Marty and, you know, highlighted, and a part of that, I think, is that, you know when information was mostly on paper, individuals could physically control the paper on which the information was contained. And so the law recognizes right of control in the paper, as within individual's private property, privacy became associated with that idea of control or property. But in a world of computerized data, particularly when computers connected to one another in networks, unit I laterally individual control ceases to be possible.

And so when the information practices that were discussed a little earlier, and the principal two people who developed them were Willis Ware and David Martin, they rejected the idea of privacy as a function of individual control, but they said it had to be an attribute of the relationship of trust between the individual and the organization.

And that recognized that the organization and the individual both have a strong interest in the proper handling of the information about the data subjects, okay? So the FIP, the fair information practices, have a normative structure where both the individual and the organization have strong interests in doing what is required.

So it's about a mutual relationship, or a mutual trust structure.

I like to talk about the privacy act, that's implementing the real idea under -- and, of course before I do that, you know, the -- the European data protection context is at some level, may recognize -- it has been largely focused on this idea of privacy or data protection or control. But when they implemented the original ATW report which was where this idea

of fair information practices came from, they -- the act did not use the concept of individual control. It used a very strong but flexible concept of compatible use, requiring information to be used only in ways compatible purposes for which it was originally collected. No surprises, right?

So for data that was not within a compatible use or otherwise specifically excluded by the actor, prior written consent was needed from the individual. So that gave a lot of flexibility to government agencies to use information as appropriate, consistent with compatible uses, but it also prevented the act from over relying on individual consent which if you require consent for everything, you turn the whole process into a meaningless check box process. So what you really there want to do with a statute is have a flexible process that can be complied with by organizations that are responsible for maintaining trust, and most organizations have an interest in using information appropriately, because it's just as much in their interest as it is in the individual's interest.

So, you know, the problem with the idea of ex-ante individual control or content is not just you end up with check box consent problems but you often end up in situations as we have seen in Europe, where the compliance rates become just abysmally low.

And small and medium sized businesses, the estimates is less than 10% of them are compliant, and really that's most business. So if less than 10% of those after three years are complying with the statute, that's one good way of losing trust, which is not doing what the law requires you to do.

On the other hand, if you can comply with the law and build trust, then -- then, you know, you are moving toward the goal, the ultimate goal of any privacy statute, which is to maintain trust between the organizations and the individuals, particularly in a consumer context.

>> STU INGIS: Great. Thank you for that. Go ahead,

Marty, you can go ahead and respond.

>> MARTY ABRAMS: So the concept of compatible use is a very broad concept. And who interprets what is a compatible use? And how do you interpret what is a compatible use? And how do you demonstrate that your process for defining what is a compatible use is part of -- of the conundrum that we face in terms of flexible privacy law? So Peter, I absolutely agree with you that flexibility is important, that trust is important, but there needs to be some mechanism for -- for organizations to -- to demonstrate that what they are doing with data is in the context of the relationship between the organization and the individual.

And that's where the concept of accountability comes into play because accountability is about the responsible and answerable use of data.

And responsible means using data within the context of the relationship in a manner that takes the other stakeholders' interest into play. Answerable is demonstrating to others that you have done that with competency, and integrity. So the question is: How do you build based on, you know, Peter saying that compatible uses is -- is a freeing mechanism? How do you build that in so that it's a trusting mechanism as well?

>> PETER WINN: Okay, I will quickly answer, but I think other people will want to respond. But Marty knows that the privacy act creates the flexibility through what are called routine uses, which are controlled or limited by compatible uses.

So if an agency gets a little greedy in how they frame out their -- their routine uses, courts can always determine that's not compatible. Okay?

So there's a court oversight structure and the privacy act but there's also an administrative procedure you have to go through in order to be able to develop a compatible use, or a routine use.

But I will defer to -- I think Jane may have some ideas

because the statute she's worked on heavily relies on that same kind of structure but in the commercial context.

>> JANE BAMBAUER: Yes, I think the USC act takes up this idea of compatible use, but I would say it actually -- its definition of compatible use might sweep a little broader than the privacy act, in the following sense that it attempts -- so first of all, let me explain that. The benefit of recognizing a large swath of compatible uses is to minimize -- is to limit the context in which you need to get user consent because consent is where there is this notion of control, and it's expensive to comply with, but also it puts a lot of burdens on the end user themselves to figure out what the likely benefits and harms of any processing will be. So the goal was to have a fairly broad context where a firm can feel confident that what they are doing is going to be seen as a compatible use. And there are two routes to showing or to proving that you are -- that what you are doing is compatible. One is the one that Peter mentioned is most familiar from the privacy act which is routine uses, something where a reasonable user who is interested and concerned about -- in this area would have an expectation that their data is going to be used in this way.

Which doesn't necessarily mean that it's -- it's exactly the one and only purpose for which the data was originally collected but it's become routine. But the other method that I think is quite important at least conceptually, and probably practically as well, is if a use is novel and unexpected, but it has clear benefits to the user, to the vast majority of users.

And I think -- I think that it's quite important because one of the downsides to a European-style or user-controlled method for protecting users -- personal data is not only that consent is expensive, but it is a true innovation killer, right? There are going to be beneficial but initially strange repurposes of data that our entire Internet economy has been built on to some extent.

And by the way, by these privacy laws that we're contemplating in the US, they are going to restrict, you know, American companies, but I'm still quite confident that China and other countries are going to be innovating big time, in NAI, and so the real question -- and once we see, you know, the utility of these applications, we will definitely adopt them, just as Europe adopted Facebook and other definitely privacy invasive technologies that American companies developed.

And so -- and so this -- the ULC bill tries to ensure that a large amount of innovating can go forward without user consent as long as there's a reasonable basis -- you know, reasonable basis to believe that the user will benefit from the new use.

>> STU INGIS: So --

>> JANE BAMBAUER: The accountable question is harder.

>> STU INGIS: One of the challenges and I will come to you, Jennifer, maybe on this one, but one of the challenges, of course, as you start thinking about what's a routine use, a compatible use, or a consumer expectation is not all consumers are created equally. They all have different views and different perspectives on the approach. And which I think has been in large part a challenge in enumerating, you know, some finite set of appropriate or inappropriate uses.

Jennifer, how do you think about that? How should -- who should be making those determinations? Should it be left to the business to figure it out and making the case? Should it be prescribed in some specific law or should it be, you know, subject to a consent or consumer choice?

>> JENNIFER HUDDLESTON: So I think there are a couple of things at play there. I think first as Jane mentioned in her comments, we can't ignore that there are beneficial uses to data. We can't just focus on the harms that are used. There's a lot of benefit to a data rich society that many of us enjoy whether we are putting it in those terms or not.

(Change of captioners)

-- how should or who should be making those determinations? Should it be left to the business to figure it out and make the case? Should it be prescribed in some specific law, or should it be subject to a consent or consumer choice?

>> JENNIFER HUDDLESTON: I think there are a couple of things at play there. I think at first as Jane mentioned in her comments, we can't ignore that there are beneficial uses to data. We can't just focus on the harms that may occur and we also have to recognize that there is a lot of benefits to a data-rich society that many of us enjoy, whether we're putting it in those terms or not.

So, when we're looking at when should privacy actually be regulated, often times what we want to look at is when is a harm actually occurring that we can all agree is a harm. So, to the example that was given earlier with the fair credit reporting act, there is fairly easy could go analyzable harms that people would say that's information that needs to be regulated. When we look at other history of privacy laws in the U.S., often times they're dealing with these subsets where there is at least general agreement that even if there is a tradeoff to innovation or to speech, that the potential for harm or the actual harm is so real and so irreversible that we're willing to make those tradeoffs.

The problem is that once you get passed a few very specific things, we have a very wide range of preferences when it comes to what information we do and do not consider particularly sensitive, so you see this in people's individual express preferences when it comes to what social media sites they may use or what information they may give out about themselves, but you also see this just in terms of how we define different types of data, what we, for example, might define as health data can vary from individual to individual.

So, when we're looking at policies that may regulate those transaction, we really want to look at those places where there is generally an agreed-upon harm and make sure that we aren't just going to the most privacy-sensitive option all the time without weighing those potential tradeoffs that may occur.

There is an important role though for education, both for consumers to educate themselves to make sure that they are acting with those privacy preferences, as well as to look at where are places where we can help to improve digital literacy, where we can help people understand what the ranges of preferences are, and why they may or may not want to make certain choices.

>> STU INGIS: Thank you. Curious maybe for any of you, if a consumer decides not to have information collected or used, but it's been shown that the ability to collect or use that information does benefit the consumer, should that choice exist?

>> MARTY ABRAMS: So, the concept of knowledge creation is an incredibly important concept, and that is really what drives innovation. Increasingly as the nature of statistics has changed over the long period, Stu, when you and I have been doing privacy, the fact is that the correlations that come with data help give us new concepts, new insights, generate new types of data based on what happens in the analytics. And the creation of knowledge is an area where there should be great liberalism, and the fact is that when we think about things like disease abatement and better education and even congestion relief, the ability to do knowledge creation is incredibly important.

Part of what the GDPR got wrong is that it precludes knowledge creation. It has a fear of the term "profiling." It looks to the outcomes once you use that knowledge rather than looking at the creation of the knowledge itself. So, the fact is that you can structure privacy law so that it differentiates from the creation of the new knowledge and the application of the new knowledge. And part of what we need to do is to think about privacy legislation that links the risk to individuals with the use. So, the creation of new knowledge is one type of use and the application of that new knowledge to make decisions about people is another, and the types of risks associated with them are different. We need to have a way of differentiating that.

>> PETE WINN: If I could jump in, and this is a fabulous conversation. More generally, and I think the answer to the

question I think is not just that it's a good idea to use things that people might not have thought of or necessarily always agree with, but there is a difference between a subjective trust or subjective concept of what the individual prefers or cares about and the objective question of what's appropriate in terms of uses. Okay.

So, the individual control model that we've been talking about associated with the GDPR assumes and is tied up with the idea of a subjective -- you know, a subjective determination about what is and what isn't, you know, an appropriate use. But, in fact, we all know that an appropriate use is what we as a society, or at least all the stakeholders in that community determine is appropriate or not appropriate. The individual control model ends up assuming an adverse relationship between the organization and the individual, and that means that privacy governance, you run into this social trap, that apps in some form of intervention by the state, administrative agency or a court, the underlying resource, that is personal data, is going to get overused or misused or destroyed. But in connection with privacy governance, this narrative, this tragedy to the common narrative is misleading. You know, it's important that there are a lot of connections with the environmental world, and famously the economist Elinor Ostrum who won the Nobel Prize for confirming state intervention is needed to prevent what we call the tragedy of the commons, that what she recognized and won the Nobel Prize for is that common pool resources, and she focused primarily on environmental resources, but also public resources like law enforcement. And likewise, in the digital world these exist digital data in which two or more stakeholders have a common interest. And what she discovered is that you can actually have humans get together without state intervention to develop effective rules to manage these resources, and when these self-regulating structures are in place, the compliance rates are very high. They have high rates of buy in, the enforcement rates are low, and the guidance is generally clear. You get high levels of social trust. And then she also recognized

that, you know, and of course the state needs to recognize these things, but if you try to control them by the state, you'll destroy them. When you see a lot of these kinds of structures reflected in effective governance structures, and interestingly David Martin, one of the authors of the FIPS was the actual designer of the Cape Cod National Seashore, which was a predecessor of a lot of these environmental laws, and so the multistakeholder organization structures are actually structures and vehicles that can actually provide high levels of flexibility, high levels of mutual control by the stakeholders, but no individualized control so that everyone gets what they need, but nobody necessarily gets everything that they want. So, in general, ideally, you want to have a privacy law that facilitates these types of structures that can be designed for particular contexts imply general principles that the statute would have, could be overseen by an agency or a court, but effectively allow flexibility, allow structures of trust building, but don't try to say that any individual gets to determine or have the final say over what can and can't be done with, quote, that individual's data.

>> STU INGIS: Thanks, Peter. A thoughtful historical context. Anyone want to respond to Peter before I move on to another question?

>> MARTY ABRAMS: Just one quick point. The General Data Protection Regulation actually talks about that the data must be processed lawfully, fairly, and in a transparent manner. It is the interpretation of the permissions that are in there that have become -- that have driven GDPR to be almost completely consent based. It wasn't -- it isn't the nature of the theory behind it. It was the actual application, and I think that's important. We tend to run to this concept of individual control when we think organizations are irresponsible in deciding what is lawful and fair, and I just wanted to add that to Peter's comments.

>> STU INGIS: Thanks, Marty. I'll maybe chime in with a comment even though I'm moderating specifically on this, but you know, I think both Peter's point and Marty's follow up, there is an

effort I've been working on called Privacy for America and we've developed a model similar to -- in a model way that the others on this panel have done. But one of the things that we really were focusing on in there, and I think it goes to what Peter was describing is to try to get away from that interpretation found in the GDPR, which we kind of call the old paradigm which is just transparency and choice, and move it much more toward what Peter was describing as appropriate uses and kind of normative standards that are evaluating benefit to society.

And so, it's interesting because the two models seem to be, you know, if you bookend them, you know, there seems to be this back and forth about what should be the model and is there some way of doing both. You see them kind of almost -- like there is a tension that I see developing about around them, so it's interesting. So let me take that and turn around the question and get into how we have the state and federal models and we talked about the GDPR and some of the uniform commission and Marty you've got a framework and all of you have worked a lot on frameworks. What's working? You know, what model should be the model in the United States?

>> JANE BAMBAUER: Before we do that can I say a little something about the range of appropriate uses?

>> STU INGIS: Yeah, please.

>> JANE BAMBAUER: So, in principle I agree with the consensus that seems to be here that -- that regulation should be trying to foster appropriate uses and try to disincentivize or reduce inappropriate uses and the ULC draft does that and carves out this zone where it's not clear that there are going to be benefits, so therefore that's the area where consent is relevant.

Now, I'm going to take off that hat though for a second to argue against going too far in that direction too quickly. Because that question still will tend to allow -- you know, tend to import general anxieties about new technology that appear generation after generation, and so if anything, there might need to be a thumb on the scale in terms of allowing even some of what temporarily looks like inappropriate use in order to see what actually happens. And

to give a historical example -- well maybe both a modern and historical perspective, right now I think there is a consensus that facial recognition is a technology that should just be off the table and that's just inappropriate, or at least in many of the contexts in which it's used right now. But that, I worry about a consensus building around even that position as unpopular as my questioning it, the or the orthodoxy is going to be because a hundred years ago or more than that when they were writing about the right to privacy, the core technology that drove them to write that article was the hand-held camera and almost all of the arguments that you hear about why facial recognition is so inappropriate can be used just effectively with just changing out a few words to describe the innovation of the camera.

And so -- and so I think that we are -- I think that we need to start thinking about what fairness means in a data-rich environment, and I applaud Marty and everyone here for starting to think through that, but I'm not sure that it's entirely ripe.

>> STU INGIS: And I think that's a really astute point and I kind of jokingly call that, you know, I critically sometimes say we've got to appease them, and isn't the challenge where Peter started if you don't have the trust in the system where the standards are, then the standards don't carry any weight.

>> MARTY ABRAMS: There are international examples that are actually interesting. They might not be the ones that we look at though. Singapore recently revised their privacy law to really liberalize the ability to do knowledge creation and think about data, and that was an intentional development. But before they actually developed the exemptions from concept that are the basis for those changes in law, they actually pushed this concept of what it means to be a responsible organization, and then they -- and they limited the use of this really flexible use of data for knowledge creation, not based on concept but based on an assessment of the benefits to individuals as well as the risks to individuals, and they base that on organizations having processes in place that could be overseen in an effective manner. So, you know, if you don't have

something that gives some framework and substance and control, then you have this risk that crazy people will do crazy things with data, and not just the thinking of the new ideas but actually applying it, for example, facial recognition in an inappropriate way. Those of us that have gone on to an international flight and been validated by our face to get on to that international flight, and I know we haven't been doing the flights lately, but to get on the plane, understand that facial recognition in that application makes a great deal of sentence. You can't make these blanket things that technology is bad. You've got to have these means for -- for establishing where they're right and wrong, and you need a mechanism that does that in a trustful fashion.

>> JENNIFER HUDDLESTON: But I think to the point, we've seen these technology panics over time and it was caller ID privacy and so when does regulation -- when is it needed a as to when which can allow the norms in society and allow some that have panic to perhaps subside as we see the beneficial uses like being able to get on a plane without having to scan.

>> PETE WINN: Real quickly if you don't mind, obviously, the FBI developed some of the more, and this is public, more of the uses of facial recognition technology in connection with the old mug shots where they're using facial recognition when they have a suspect for kidnapping a kid or committing a murder, they don't know who the suspect is, they run it against the existing mug shot list and generally speaking we've got a whole lot of controls and protections to make sure that's not going to get misused, but those are not the typical examples that people are concerned about when they're talking about, you know, the risks of facial recognition technology.

So, obviously, I agree with everyone that we have to be careful before we ban a whole technology, and we've often argued for the appropriate use of facial recognition technology by governments, but at the same time we work -- I work in a country, in a government that's elected by the people and at some point the people get to decide these kinds of questions about how certain

types of technology can and can't be used, particularly by their governments, where we don't have first amendment rights that might limit what the law can do vis-a-vis what the private sector does.

So, it's always important to keep in mind that the solution is that we've got to educate people enough so that appropriate uses can be allowed both by the government and by the private sector, and at the same time recognize some deference to the fact that the legislatures can get it wrong sometimes because that's why they're democracies.

>> JANE BAMBAUER: Yeah, and maybe an example very quickly of a use of sort restriction that we're quite accustom to is anti-discrimination law, in which Title VII can be thought of as a data governance law and disallows certain uses of information that a company might have at their disposal, but cannot use to make certain determinations. But that's an example of something where a problem emerged and then a discrete solution was crafted, and so I guess an open question is whether it's better to let law lag and see where we go and then play wack a mole, or whether there are some principles that we feel so confident are going to apply long term that we can do the sort of division of good and bad uses in advance.

>> STU INGIS: Yeah. So that is the question from my perspective. You know, I think things were working pretty well. You had statutes that had been passed over many years where there had been real threats and harms and the Internet was booming, and we had good self-regulation along the lines of what Peter was describing built in, and now, you know, we're seeing in the U.S., you know, I think we have three or four state laws this year and another one a year or two ago, and so what's working? What should we do? We're now at a stage where we're starting to get some conflicting laws, we're not even clear what approach we have, we're not clear who gets to write the laws. Some real estate developers in California think it's them, and we each think it's us in our own way, and I say that jokingly, same about the real estate developer. But the Congress certainly, you know, is a channel, but so what do you all think? What should we be doing?

>> PETE WINN: Can I jump in before everyone? I just want to highlight the difference between a general data protection or comprehensive data protection law and sectoral law and we have laws like HIPAA and others, and they're probably -- I mean they're probably just like over 200 or 300 state and federal privacy laws that govern particular sectors, and nobody is complaining very much about the protection that's taking place within those sectors. So, it's always helpful to keep in mind that are we asking about a law that's going to just take care of everything and replace the sectoral laws that nobody is complaining about, or are we talking about filling in the gaps where there has been a breakdown in trust, so that's sort of the question I would sort of frame up.

>> STU INGIS: Good. I like it. Marty and then Jennifer.

>> MARTY ABRAMS: So, I recently had a conversation with a senior European official in private, and I said one of the things that happened with the GDPR is that there was a decision that it would be risk-based legislation but nobody ever discussed risk of what. So, you've got legislation that on the part of European regulators is risk that individuals won't be able to exercise the rights to object, for example, for flexible uses of data. And while the business community thought it was risk of real tangible harm, and oops we got it wrong. We passed the legislation that's risk based and never asked the question of risk of what. At the IAF, the organization I run, this is one of the basic questions that we think has to be --

>> STU INGIS: Marty, just to be clear. It wasn't we who got it wrong but it was "they" who got it wrong.

>> MARTY ABRAMS: Put it this way. The collective community of mankind interested in European law, they got it wrong. So, the fact is that in California, I don't think there was this question of risk of what. I can tell you based on what I read in the Virginia law, there wasn't that question of risk of what. There was a requirement that you do risk assessments but never defines risk of what you're doing risk assessments for. So, you know, I think a really important exercise is defining risk of what, and I IAF

legislation fair and open use act, we started with the question of what are the risks that we're trying to confront, and its negative outcomes of using and not using data. It's both ways. It's both the decision not to as well as the use-to-use data. And we begin to describe mechanisms for assessing the levels of risk, so -- so, you know, I will tell you we're going to do a program if Washington DC and have people begin to debate the concept of risk of what, because I think it's a basic piece to not making the mistake that was made in Europe where they created a law that is, quote, risk based, and there was no agreement on what risk based means. I'll be quiet.

>> JENNIFER HUDDLESTON: I want to jump in on the state-by-state approach and some of the risk associated with that kind of patchwork that is starting to emerge. So California, of course, kind of had the first move as a large state with many tech companies in it, and I think there was a sense that in some ways the CCPA and now CPRA has become de facto Federal law and the question is what does that mean for those of us who don't live in California who may have different privacy preferences, and what does that mean with several elements of this law that were not fully interpreted at the time that the law became effective, and now that you've had further dramatic changes of it. Then you start to have other states pass these laws, Virginia being the most notable one this term that has a different model than CCPA, but you've also seen states like Nevada pass one, Maine has a different one involving primarily ISP-related issues. But you start to have this patchwork emerge that can create confusion, not only for businesses that are trying to comply, but also for consumers about what their rights are and what risk -- or what's considered risk or what's considered improper use. I do think it's interesting when we consider, say, the uniform law commission approach or this kind of question of what if everyone just passed their own version of CCPA, would that be better to have 50 states with their own individual law that looks almost identical or a federal law? And if you have 50 states even with their own identical law, you're certainly going to get different interpretations by Attorney's General over some often very key terms

to consumers and to companies trying to comply, and what does that mean as opposed to a Federal Law, let alone if you have 50 states with 50 different laws and some of which are inevitably going to conflict with each other.

>> STU INGIS: It's interesting that the collection of online data in particular, you've got two laws in Europe, the GDPR and the Privacy Directive. You've got the various laws, including this new privacy control that was self-created outside of the statute and the CCPA which will be taken away by the CPRA. You also have the Apple law, their standards. You've got the Google standards. So, how is a company to comply, and what's a consumer -- you know, what's happening here?

>> JANE BAMBAUER: Well, so in terms of how the company must comply, I mean, companies are going to have to comply with the intersection of all the strongest laws in which they operate, and the Uniform Law Commission, by the way, we did not take it on ourselves to have uniformity across the state as our main goal, and instead we favored interoperability so that if you're already complying with California, you will automatically be found compliant with this law that we put forward. I agree with you, Jennifer, that ideally, we would have a federal law that is a gap-filling law between the -- for the sectors that are not already -- that don't already have their own federal law, like HIPAA, and it would be different from GDPR. It would, being the global model that is workable and that reduces risks of harm, you know, concrete harm as Marty referred to, and it winds up not looking very much like California's law, which I -- you know, at least I think could not possibly survive a first amendment challenge when they inevitably come --

>> STU INGIS: Totally agree. You know, it's interesting that you're also about to see -- you know, as clients ask me how do we comply and what should we follow and what's going to happen, my kind of constant refrain is that it's going to get a lot murkier before it gets cleaner. Because you're going to see even more and more of these different state different approaches. I thought I would

mention and see if anyone has any thoughts on this, but it appears that the FTC is also picking up its pen now or picking up a pen that probably they don't even have authority of, but to dive in, you know, you read the tea leaves through the Executive Order and some of the new changes of the chairwoman there but as I read it they're about to write a privacy regulation which wouldn't be preemptive because the statute is not preemptive in which they tied into, so I'm curious how is that going to play? Any thoughts?

>> MARTY ABRAMS: So, we've had an unfairness -- first of all I'm not a lawyer, Stu, as you know. So opining.

>> STU INGIS: You know more than lawyers I know.

>> MARTY ABRAMS: We've had a lot of unfairness in the United States and there is a concept of fairness that exists in other jurisdictions and I'm not quite sure how the Federal Trade Commission moves from what is an established unfairness concept under Section 5 for a general concept of fairness that you have to provide fairness and describing what that would be. So as a nonlawyer, I just don't see how you make that jump. And we've had this discussion about going from an unfairness standard to a fairness start for 25 years, Stu. And there are reasons we haven't made it. So maybe I'm a little bit of a --

>> STU INGIS: So as a legal matter I totally agree with you. I'm just reading the tea leaves and telling you I think you're going to see a proposal that's deeper than all the ones we've written combined. That's my prediction. You heard it here first.

>> JANE BAMBAUER: Well, and it will be really interesting, if that happens though, it's going to be interesting because another -- you know, another goal of the FTC is to promote competition and the more complex the concept of fairness is the less competition we're going to get when only Google and Apple can comply, and Amazon I suppose, and so I don't know how they're going to responsibly manage those two goals that can be an intention.

>> JENNIFER HUDDLESTON: If I can jump in here. You know, similar to what Jane was saying, I think we also have to discuss this intersection that often occurs of when you have very complex

data protection and privacy roles, it is the largest players who are often able to comply with them, and the cost of compliance, the burdens of compliance on smaller players, on innovative startups is and can be incredible, particularly when you look at something like California's law or like GDPR, not to mention non-tech companies often subject to these requirements.

I also think when we're talking about the FTC's role in this, it's important to look at the ways the current system has worked. The FTC has been an enforcer on data privacy issues when there has been consumer harm involved, and so we need to look at that question of, you know, if we continue to focus on what consumers experience, and on those cases when there is actual consumer harm, there has been advantages to this permissionless approach that allows these new innovative companies to get started without a lot of regulatory red tape and potentially challenge existing giants.

>> PETE WINN: If I could jump in real quickly. I want to say two points. I agree with everything that everyone has said, and I want to focus on just this sort of experience in Europe for a second. One of the things I've observed is that when you actually look at the difference between law on the books, at least the books in breakthroughs and law on the ground enforced in member states, you end up seeing what is effective sectoral system as well, because it's ultimately going to be -- the law is going to be complied with and where there is any reasonable chance that it's going to get enforced, and for small and medium-sized businesses in Europe, it's not going to be enforced.

Now, and you can see that some of the data protection authorities, the McNeil in France, Helen Dickson in Ireland and Liz in England and will list what they're going to list as priorities. They say health care, finance, and employment, and they're all going do cookies. There you are. And the danger with the approach -- the reason they do this is they go to the legislature the parliaments and have a conversation about what it's going to be and how much money they're going to get and the parliaments appropriate what they want them to enforce. Okay. In some

European Member states, my budget at the Department of Justice as the privacy officer is bigger than the data protection authority's budgets in places in Europe and I will not tell you we're 100% compliant but we're working on it, but the challenges of dealing with 600 or 700 systems versus millions of systems, you can sort of see the real compliance we're going to see there and that's fine. Can you have a sectoral system based on pure administrative discretion but that's highly problematic in a democracy and it's highly problematic in a country like the United States where we generally expect laws enacted by democratic legislatures to have a tendency to be enforced. So, I'm sort of repeating what everyone is saying, but you know, you know, you cannot look at a statute like the GDPR and say that it's a comprehensive privacy law because it's not. The reason that everyone -- you know, this creates the illusion of one, but the reality is that it's sectoral and the reality of any comprehensive privacy in the United States is sectoral to some extent but we like to law to reflect it's not going to be a one-size-fits-all solution, otherwise you're going to have a situation where it's kind of like a social trap and nobody actually believes in the law and it undermines not only the rule of law but trust more widely in the government and social society.

>> JANE BAMBAUER: Peter raises a general problem with law which is that when it is too aspirational and too harsh, then it becomes a law of discretion and everyone is trying to read the tea leaves to figure out how it's going to be interpreted and enforced. So, another way of putting that, though, is that I think a feature of a workable privacy law is one that has a process that allows for safe harbors to emerge as we learn how technology works and what its impact is. So, I guess, you know, the silver lining to the FTC maybe wanting to get more involved is that they would be a good regulatory board for developing safe harbors if that's the kind of, you know, notice of the features of data processing that are per se legal, and the ULC draft has a process too for sort of stakeholder engagement-based, voluntary consensus standards to be proposed and then eventually adopted.

So, maybe tying all of these threads together, it may be that what we need for functionality is not only at least some clear examples of forbidden processing, but also some nice clean examples of data processing that maybe we didn't think of initially but we now recognize as safe enough.

>> STU INGIS: Yeah. Interesting. Outside of the question of legal authority, I kind of share what I think I heard -- like the FTC would be particularly at the staff level where they really do know this stuff in and out, would be a thoughtful organization to write rules. The challenge, though, is if you can keep it from being politicized because the way I'm reading it, it's basically like, you know, a senator deciding by themselves here is what I'm going to do and here is going to be the law. That's not going to -- that dog is just not going to hunt. They're going to learn quickly that there are three branches of government, but that's just my side editorially.

>> JENNIFER HUDDLESTON: I should say I think on that notes it depends what exactly we're talking about the FTC actually doing, are we talking about the FTC right now with the current authority deciding to issue a completely new set of privacy guidelines or are we talking about a situation where in developing a data privacy bill the Congress delegates certain elements of that bill to the FTC in their capacity as a consumer protection organization and given their experience and expertise with enforcing other existing data law.

>> STU INGIS: Here is my prediction, which is I don't think it will come from -- I think it will come before Congress would act. But I think it will be similar. And this may be attractive to some people, but when the do-not-call and telemarketing legislation was rolled out, it was 60 pages of regulation without authority and the Courts found that it had no authority. And then the Congress gave them the authority after the fact.

But to me I think that's what you're going to see. I think you're going to see a very progressive, as if it were any of your favorite progressive senators, some who I love and I love their ideas, so I don't mean any of it as critique, and it might actually

be a very healthy thing for the country, but I think it's something that should be on people's radar as I'm starting to read tea leaves here.

>> JENNIFER HUDDLESTON: And, of course, then --

>> STU INGIS: I'm sorry, Jennifer, finish and then Marty.

>> JENNIFER HUDDLESTON: I was going to say, of course then there gets to be some very interesting administrative law questions that are beyond the scope of this panel.

>> STU INGIS: Totally agree. Yep. Marty?

>> MARTY ABRAMS: So, let's go to some of the things that are going to happen. We're going to have a greater emergence of artificial intelligence in the United States. It's just going to happen. We're going to spend more time bringing data together to think about the insights that that data gives us. That's going to happen.

What is important is to make sure that we have some boundaries in which that can emerge in a thoughtful way where the negative impacts are thought through by parties and can be overseen by responsible regulator and overseers.

Putting the FTC in the position of making law because we don't have law, to me, it's not the most productive way of doing it. And being afraid of data being allowed to give us new insight, which I can't predict what those insights are going to be, is also not great. You know, we talked about oh, we've got -- we've got sectoral law that's worked well, but well the HIPAA precluded a lot of health-related research that would have been very useful because of the way it was structured and interpreted. So, the fact is that we need a mechanism that allows for the making our lives better with data to emerge. Yeah, there are going to be some negative consequences where things are going to be thought of as stupid, but we need some boundaries to let that emerge in a thoughtful way. That's what I'm suggesting privacy law should do, is create the boundaries for us to think with data to create new insights to allow innovation to occur and to do that in a way that has boundaries overseen in an effective way.

The FTC has 40 to 60 people doing privacy rights, Stu. It's tiny compared to the number of people at the ICO who are doing privacy which is probably 500 or so doing it. That's not a prescription for an effective oversight agency, and giving them -- you know, and just I think we need to have some structure for that to emerge.

>> STU INGIS: Of course, if any of these -- you know, if the new budget gets passed, they may rival the ICO fairly soon. So, we're at about 5 minutes left, and I thought it would be a good opportunity to give each of you a minute or so plus to add anything else. Where do you see the world going? But to just kind of tie some of your thoughts to have a final thought here. I'll probably have one last thought to tie it up at the end. I'll start with one now. I would delegate to the four of you, and I'll probably try to chime in too to pass the law. You all can right write it and I think it would be good and we'll be in good shape. I think it would be a good product. Peter, let's start with you.

>> PETE WINN: Well, I'm not sure I have a whole lot more to say. I guess the key issue for me is if you're going to enact a law, is it something that the regulating community can actually comply with? If it's not, stop and do something else. If they can't afford to comply with it, they won't comply with it, and then you're going to be kind of playing the kind of games they're playing in Europe, which frankly I think result in a loss of social trust. The key here is to come up with a structure, a legal structure where the business community, which is going to be asked to comply with these laws, has to be able to afford to comply with them, and that is the first question because, you know, how you get there, but to date with the possible exception of the uniform law commission statute, which seems to be a much lower-cost vehicle, I'm not sure I've really seen -- or sector-specific structures like, Stu, the privacy for America thing that the largely advertising folks put together, which is sector specific.

>> STU INGIS: Right.

>> PETE WINN: But, you know, within a sector you can actually

design these things that are detailed and specific and you can afford them because everyone in the sector knows what the rules are. But if you're going to have a comprehensive law, you can't do that level of granularity. You know, the uniform law commission has the general rules and then it allows the voluntary consensus standards to develop the sector-specific structures that would be more specific. But absent that kind of iterative process between the sectoral specific process and the general rules, I don't see any other alternatives to something that's affordable. And without something that's affordable, you're going to have a privacy law that destroys trust because then all the people that are supposed to be complying with the law won't be able to afford to comply with it, except the large companies like Microsoft who already have built in to that structure, and it's just going to result in anticompetitive advantages for the big guys against the little guys.

>> STU INGIS: Great. Thank you, Peter. Jane?

>> JANE BAMBAUER: Yeah, so let's see. I think the features that we should be striving for -- well so first of all, on Marty's last parting thoughts or the last set of thoughts, I see the first amendment as being the backdrop along which we should train our privacy laws, and if you adopt that vision, then there is already strong protection no knowledge creation and there is a requirement that whatever law be enacted be fairly narrowly targeted to a concrete harm. And that's great, it's just if we can comply with the requirements of the first amendment, then it's going to be a pretty good privacy law because what it should be doing is prohibiting or restricting to consent procedures, the risky things that cause concrete harm.

And then outside of that, outside of that, I think that the old system that everyone hates right now actually functions pretty well, and the old system being transparency for consumers with a basically take-it-or-leave-it deals. And I know it seems like it's not in consumers' because if they don't want tracking and behavioral advertising, it's very difficult to avoid that, but at the same time if consumers really understood how much of the World

Wide Web and parts they like the most, how much depend on behavioral advertising and the bump in revenues that they get from it, you know, if we can see the alternative universe where there really isn't behavioral advertising, it's not clear that consumers actually want what it seems at least superficially they want today.

So, I'm comfortable saying that we should be looking for -- looking for relatively narrow ways to prevent concrete harm.

>> STU INGIS: Great. Thank you. Jennifer?

>> JENNIFER HUDDLESTON: I want to echo a lot of what Jane just said and I feel like that's something that we haven't really dove into in this particular panel, that when discussing privacy, it's so important, these points of friction and tradeoffs involved with privacy. It's, you know, privacy is one of those things, kind of like puppies that everyone is for it and very few people will just be like I'm an anti-privacy person. (Laughing). But when you actually boil down to it, there are a lot of points of friction, whether it's questions about the right to be forgotten and how that can impact freedom of the press and free speech, whether it's questions about data and speech and the first amendment, whether it's questions about the impact on innovation or smaller companies in competition. I think we can't just say that privacy is good and therefore privacy should always be our north star. We've got to very carefully examine the tradeoffs and really take them into account in any potential privacy or policy we may be creating.

>> STU INGIS: Marty, we're at time but why don't you have the last say.

>> MARTY ABRAMS: So, the fact is that recital for the GDPR says it's all about the full rights and interests of people, and they just ignored that when they wrote the rest of the law. And I think that we all have an agreement on one thing that's very important, which is knowledge creation is where innovation comes from and that we need to have privacy law that is protective of people but a allows for the free expression that comes from combining data in interesting ways to come up with new insights.

>> STU INGIS: Great last word. I think we can all agree to

that. Thank you all. This has been a terrific panel. Please join me in thanking our great panelists, and let's do this again. It was fun. All right. See you.

>> PETE WINN: Thanks.

>> DUSTIN LOUP: All right. Thanks, everyone, for a fantastic panel. We're going to move into a quick break here and we will be back at 3:00 eastern time sharp for a discussion on antitrust, and then immediately following that we'll move into the discussion on scenarios for 2026 and will everything work everywhere and discussion on potential Internet fragmentation and how to avoid it. Enjoy your break and we'll see you back soon.