2023 TPI Aspen Forum
Whose Data is it?

Jeffrey Prince:

Things like that, that we can benefit from giving up our location data, all of a sudden the trade-off might've fallen in the other direction. So can you go to the next slide, please?

Shane:

Oh, are you saying, oh, do I have it?

Jeffrey Prince:

Oh, I don't know who's-

Shane:

Am I in charge this whole call? I did not know it.

Jeffrey Prince:

Sorry, Shane.

Shane:

Look at this. I'm in charge. Whoo.

Jeffrey Prince:

Briefly, a very quick takeaway here is what we found is the relative valuations of data is incredibly consistent across countries that we looked at. So by no means do I expect people to process everything on this slide, but if you just in your mind, look at the relative rankings for all the different data types across all the different places that we looked. So here you can see the different types at the bottom. You can see the different platforms where we asked about people's willingness to give up those data. It's almost perfectly identical across countries in terms of the relative rankings, which I think is a striking finding.

Next slide, please. And just, I think out of interest, we did some demographic cuts. You can see that there's significant differences in willingness to accept, to give up their data across sex and age, not so much by income. You have a little bit there in terms of balance, but otherwise it's actually quite consistent. So you get some clear demographic predictors, but in other cases, not so much. Next slide, please.

Okay. And then I will wrap up by saying, Scott and I did a recent project that we've just put out that is focused on data localization. So data localization, as I'm sure many in this room are aware of, are different laws and policies that countries have been either contemplating or have put in place, that restrict international sharing of data. And so, one thing we were looking at is just to see, do people actually care, right? So some of the arguments in favor of data localization laws would be, "Our citizens want this, right? They're concerned about our data being shared internationally."

So what we did is basically tried to assess, do people actually care? And the takeaway from this graph, again, I know there's a lot here, but look at the blue dots in the middle. The blue dots in

the middle indicate basically, not caring. If there's a blue dot in the middle, that indicates that roughly there's no indication that there was any added concern in sharing data internationally versus only domestically. We still saw people want to be paid for their data, right? They cared about sharing it in the basic sense, but they didn't really make a big distinction internationally versus not.

And then I'll just, one more slide and then I'm done. I do not expect anyone to process this slide, but I will do, what I would do ... The only way I can get my kids to look at anything I do is to make it a fun game. So the fun game I will say here is look at the stars, look at the word that's next to the stars, which in this case is almost entirely going to be the NEG, meaning negative. What does that mean? It means that when we included this possibility to share internationally, but exclude China and Russia, people not only didn't care, but they actually preferred to have China and Russia in there, if you shared internationally. So if you shared internationally, there was an actual preference for having China and Russia included.

You might say, "Okay, how does that make sense?" Well, one, I would say again, this is cost benefit. So did people say, "Wait a minute, maybe there's a cost to me in not having say, China have access to my data." TikTok comes to mind. And the other thing that I think is interesting to flag is, and it is hard to see, I think from this graph, is the ones that showed this the most were Japan and Korea. And I think that makes some sense because you think about, they're kind of in an economic block with China, so they might be a little bit more averse to cutting them out with any kind of data sharing policies. So I know this a lot, but I will leave it there and step back for the rest of the panel.

Shane:

Thank you, Jeff. And all this is available on the TPI website, including on the appendix and all that fun stuff. So somebody else is now in charge, because I don't know how to make things. Here we go. So, Christian, I'm going to go to you, give us the international landscape.

Kristian Stout:

Sure.

Shane:

And God bless, he and I have talked for two hours, and then he walked up, he goes, "I have eight minutes?" I said, "Five."

Kristian Stout:

And I don't know if I would use liking of TikTok as a way to sell that. As a parent of teenagers, I'm constantly telling my kids they're not allowed to use it.

Shane:

But, do they anyway?

Kristian Stout:

No.

Shane:

Oh, yeah. I don't.

Kristian Stout:

Well, I control their devices.

Shane:

Oh, nice.

Kristian Stout:

Unless they get a burner. And if they got a burner, God bless them.

Shane:

You're not paying for it, so that's good. Right?

Kristian Stout:

I encourage them to wrap around efficient rules if they have the ability. So that was actually a really great transition into what I want to talk about and what I wanted to address briefly, and I've condensed it as per Shane's request. Relates to a big theme, a couple of big themes that have been in a lot of the panels here, this couple of past couple of days, which is the overlap with industrial policy and then the implications for artificial intelligence, research, and products down the line.

So we finished looking at the idea that broadly speaking, most people don't care if you localize their data around the world. But unfortunately, see a lot of countries are moving the direction of data localization, either with explicit policies or implicit policies. There are some explicit ones being enacted in countries like India, Brazil, a number of other countries. And then honestly, I look at policies like strong GDPR type of laws, or the way that the privacy authorities in the EU treat data flows as a sort of covert industrial policy in a way. And I think it's important to understand that and understand what the cost of that is for world trade, and for the interconnection of all our different societies.

So, as Jeff alluded to, frequently, there are two reasons why I think you see these data localization laws. There's the stated one, and then I think there's the implicit one. The stated one is going to be something like a consumer protection justification. Sometimes, you'll see it as, put as a national security interest, and that's the way it gets sold to the populace and that's the way it gets sold in academic circles. I think more on a deeper level, like I said, I think this is actually a form of industrial policy. It's a way of enacting trade barriers that in a way, hopefully benefits national champions. And then particularly since the Ukraine War, I think another justification you start to see sort of circulating is, this idea of decoupling from the western aligned countries that have the ability to shut down industries in countries, if we want to enact sanctions. I'm not going to say whether that's actually a good policy or not, because I'm not a national security expert, but it's frequently not the purported justification. The purported justifications are the ones that Jeff touches on.

But I think that there are big problems with having these implicit industrial policy aims that I think are necessary to take account of, particularly if the populace, as Jeff's research shows, don't really care if you localize their data. There's the basic dollars and cents issue. Just between the EU and the US, I think on the US side, the transatlantic digital trade is responsible for about $300 billion a year. On the EU, there was some research that I can share if anybody wants to see it. It's in a paper that I co-authored with PPI. The estimate is that it's something like, even moderate data localization controls in the European Union would result in about 160 billion euro

reduction in exports. And when you start to factor in all these other countries, we're talking about real money now.

And so, this is very important for these economies, but I think that the actual harms are something much larger. So for instance, data flows, the ability of firms to track data flows across borders is extremely helpful in doing things like fraud prevention, for instance, credit card networks. When they're able to look at how data transfers across borders, they're able to find fraudulent gangs of people who commit fraud, trying to figure out how to get around local policies in order to commit credit card fraud. And being able to have that sort of global view of data, enables them to build much more robust networks across the world.

Similarly, you see the ability of firms to look at cross-border data flows to optimize their networks. So we've all been through COVID recently, and we all saw how important data networks became during that period. So if you have a fractured internet where you can't actually track these data flows, it becomes much more challenging for firms that are trying to get people connected and staying online during national disasters, COVID, or war. The flip side of this decoupling argument. It becomes much harder to optimize these networks when you have these data flows being restricted.

And then I think more broadly, we need to understand that there's welfare enhancing effects of being able to utilize these data that are easy to not take account of. So there's this concept out there that I think is completely off base that data is the new oil. It's been floating around for quite a while. There's this imagination that if firms just have a lot of data, all of a sudden, they have a lot of utility. The truth is, most data is completely worthless. The problem is, you don't know what data are worthless or are worth something until you actually collect it and analyze it, and figure out where it might be put to use. It's a classic market effect of doing information discovery. If you start to wall off pieces of data into different countries, you are minimizing the ability of firms to actually do that discovery process and discover the value.

So for last night on one of the AI panels, there was someone from EU Parliament who said, "Why do you even need artificial intelligence? You have seven billion people. Just use a person instead of using artificial intelligence." Well, the truth is, you don't know what you don't know until you try to discover it. And that kind of view from a regulator to say that, "Well, we should just restrict data localization, because what value are you really going to get from?" It reflects the sort of, like a hubristic view from a regulator that we already have everything we need, and in fact we don't. We don't know what we don't know. So these data flows become very important for enhancing welfare across a number of industries.

So I'll close with one final thought. We hear a lot about the China threat. I don't know exactly how much of a geopolitical foe we need to treat China as, in terms of how ramped up our industrial policy would be. However, there is one thing that I think is important to think about in this geopolitical competition. Who develops the tech sets, the norms? If the Western allied nations have a policy of restricting data from flowing across borders, treat each other as geopolitical adversaries when we're not, we are not going to set the tone for how the artificial intelligence is developed, for how this technology is developed. Other countries that don't have the same values that we have will set those norms, and I think that's something we should take into account. Thank you.

Shane:

Good job. Thank you very much. So Tim, we're hearing that there's a lot of international challenges out here. Are we losing by not having a national privacy bill? And what are you doing about that?

Tim Kurth:

Thanks, Shane, and thank you all for having us here. I would say yes. I mean, we are seeing where US leadership has been compromised and I can kind of tell in a couple lanes of how we've approached it. We've obviously had a very extensive bipartisan data privacy arc of drafts and negotiations over the last few years, and I'll come back to that in a moment. But the other thing we did, and this started in 2020 on a number of house Republicans in our committee, where we came up with what was considered all of these different emerging technology studies and reports. What would become American Compete Act, which we have now received back just last week. It's on our website and I don't usually quote NIST, but it's on their website, too.

And one of those is on artificial intelligence. There's blockchain, and added manufacturing, some other great stuff I'd encourage folks to look at. But the number one recommendation that came back first was obviously, in terms of where our US leadership is, is enacting a comprehensive data privacy bill. And I guess I was heartened as well by hearing attorney general from Colorado yesterday talk about the importance of being like, "All right, preempt me." Like, if you can have a uniform law, that is really essential. Because what we are seeing, that companies obviously are already complying with California, they're complying with GDPR. You're already a 10th of the way through, even more. How many states were on now? Ten and counting, depending on how you define the comprehensive bill. We're losing any kind of uniformity. So the tremendous cost for American business is going to continue to grind on, and that's not going to get any easier.

And then I know in the other panel today, it kind of creeped into stuff that Jamie and I work on with the Federal Trade Commission. It's like they made a commercial surveillance rulemaking proposal, just when we were marking up a bipartisan comprehensive draft bill last year. And I don't think that was any accident. I think that Chair Khan frankly would like to preserve as much authority as she can. We want to have a prescriptive law that is very clear, not just for the FTC but for business. So they know what clear protections and what they need to abide by, and what clear protections there are for consumers. And, I think these are all great points about how consumers know the value and what's important and what's not. But I think that still goes back to what we've really tried to instill in the process early on.

We wanted to give consumers control. I mean, for our side of the aisle, that's certainly something very important, that at the end of the day, we don't talk about it in ownership terms usually. But I think in terms of personal control of what hits your kids and others, and I know Jamie's going to get into that, having this underlying comprehensive authority is going to help us on numerous levels, whether we're talking about internationally, whether we're talking about the stuff we're trying to do on kids or just ensuring like, "Hey, I think it's great, and we have really strong kid stuff in the bills we're working on." But at the same point, my guys are 15 years old. I don't want them to suddenly lose when they turn 18 or whatever age it is. How can we continue to bring that forward and so, everyone has that control? And at the same time, we have American business that can lead.

And I will just go back to our first hearing of the year, was about US leadership in a number of areas, which included whether it was enacting a data privacy bill, as well as autonomous vehicles. So again, we're talking about where we can lead on artificial intelligence. Here's a wonderful application of it. And I know there's concerns about, it's going to make news when stuff crashes, but it's like there's a lot of crashes every day where people die out of negligence. And I think that there's a great benefit for perfecting this technology here and not in China.

And I will just say, going to maybe the last hearing that we had on data privacy, one of our witnesses from industry, and he was like, "Listen." I'm like, "Our conversation amongst privacy officers goes back to, is it's like we're better off talking to Brussels or Sacramento to influence

policy." And that's really disheartening for people in DC. They run really hard to get elected and that's where the focus should be. And it's undeniably interstate commerce, and that's what we do in our committee. That's our underlying authority. So I guess I'll leave it there. We certainly feel strongly about it. Chair Rogers has been leading on this for years and we appreciate the bipartisanship, and we want to get it done.

Shane:

Thanks. So Jamie, you've been hard at work on several different bills, but talk to us about, you mentioned, Tim just mentioned that child online safety work you're doing. So, tell us about it.

Jamie Susskind:

So first of all, I should say thanks for having me. I guess the expectation is that if you put people or Hill staffers on a panel, then they're going to fight. But actually, I think our bosses, and Tim and I agree on far more than we ever sort of argue about. So they've been a very good partner in this. So yeah, I mean I would echo his sentiments. The US, we hear it all the time. I think that we are losing, that we haven't gotten there yet and we can't act soon enough to get this done.

So my boss is the ranking member of the Consumer Protection Subcommittee on the Commerce Committee. She's also the ranking member of the Human Rights Subcommittee on Judiciary. So that gives us a pretty interesting perspective, especially when it comes to China and to some degree, like how we interface with China and data flows, AI surveillance, all of those questions. So we sit in a pretty unique position with regard to all of these issues.

And I had been telling Shane prior to the panel, that my boss and I in February, so when she took back over the subcommittee and she made a very deliberate choice to take this subcommittee over another subcommittee, because these issues are really so important to her. So we did a trip to Europe, we went to Brussels, we went to the UK and we went to Dublin and we did meetings with a lot of the officials, including the Dublin, the Ireland Data Protection Authority, Helen Dixon over there. We met with commissioner, and I always say her name wrong, Vestager at the European Commission. And it was just, I mean it was enlightening both as you said, I think last night, Shane, their process is weird. So that's a whole other thing.

Shane:

I don't think I said, "Weird," but yeah.

Jamie Susskind:

But, it was enlightening because Commissioner Vestager sat across the table from us and she said, "The US, you are so big on individual freedom, but what are you doing about this, right? You're not making any movements forward, to actually get a bill forward that would protect individual freedoms to own your own data." And my boss is like, "I agree with you. We have to do," as my boss says, "More to protect your virtual you." So I think we would be perfectly happy to work with our colleagues. We are differently positioned than Tim and the rest of his staff, because we are in the minority in the Senate.

So I'm not really in a great space to tell you what the committee wants to do or plans to do on our side. Duncan spoke yesterday. You heard a little bit from Edgar, who is our counterpart in Senator Hickenlooper's office. But to some degree, I think that some of those priorities, while my boss is very vocal about, "We need to do this, we want to do this, we want to engage with you to do this," it's not at the end of the day, sort of ultimately our call if it happens or it doesn't happen. So I think we'd like to be hopeful that folks understand the importance of getting it done this Congress, recognizing that we do not run the committee and we are not in the majority.

That being said, yeah, we have tried to be still active in this space. My boss, particularly on the kids front, knowing that comprehensive consumer privacy may not, right? At the end of the day, we maybe can't be the ones to sort of individually move the ball here. So she has been focusing a lot on the kids space, which Tim mentioned, and I think Duncan and Edgar and Jeff mentioned yesterday.

So the other day, she and Senator Markey sent a letter to the FTC about alleged violations of COPPA that YouTube may or may not have been engaging in and suggesting that. And while this conference has had a lot of conversation about the FTC, and that's fine, and I think I probably agree with where most people are. But at the same time, if in fact the company is violating COPPA in the way that it seems like they may be, then that is a thing within the FTC's purview to be looking at and they should be.

Similarly, my boss and Senator Blumenthal are the leads on the Kids Online Safety Act, which has sort of come up along the edges here. I would say, we think of it as a little less of a privacy bill than what COPPA does or what ADPPA does. We think of it as more of a safety by design bill and happy to talk more about that. But we have 44 bipartisan co-sponsors right now. It got marked up and passed the Senate Commerce Committee right before we went out to August recess. I don't think that will address the broader data collection issues. It won't address the adequacy decisions that we had to talk about with the EU, and that has to be a separate priority. But obviously, we've heard from countless parents, we've heard from physicians, we've heard from educators all about problems here. And I think for my boss it was like, "Enough is enough on this front." But it doesn't negate the fact that we need something more comprehensive done.

Shane:

All right. So I'm going to move back to the international thing, but just a quick question for our two congressional panelists, because about 80% of the people in the room want to know the answer to this question. Private right of action. That was the thing that got us with Cantwell last Congress. Are we still expecting that to be a huge juggernaut, or are we even talking about it at this stage?

Tim Kurth:

I mean, we remain in bipartisan negotiations in the House. I would expect there'll be some form of a private right of action. I will just say to put it into some context, when my boss, Catherine Morris Rogers came into this, she was very opposed to a private right of action. So a lot of the things that we look at in terms of like, "Okay, if it's really about making sure a consumer has some sort of ..." "If we're talking about restitution, okay, well let's make for sure they're going to the FTC, they're going to their AGs. Is there an issue of what's available to them then?" Like, "Okay, well at that point in time then, we can kick in the private right of action."

And what we looked at in our approach and frankly our concession in this, let's make it as limited as possible. There was no statutory or punitive. And frankly, we've seen it, whether it's in the Senate, and even I'll tell you, we have some lively members in our caucus that frankly don't believe in the federal government in a lot of things, certainly not the Federal Trade Commission, and would like to give multiple kinds of private rights of action out to a consumer.

And what we're trying to find is a balance that works for our entire caucus as well as the Democratic caucus to find that balance. And I think that's why, what we saw last year was a very narrow private right of action. Only applied to certain parts of the bill and obviously, we try to focus in on where there's potential for injunctive release. So there's potential resolve issues before this somehow becoming a big thing for trial lawyers, which we sought to make sure too. Like, "Hey, if they're doing this before they're sending out demand letters, before they're

supposed to, they're going to be subject to bad faith under FTC rules, as well." That's what we're trying to find to make this whole pinwheel work.

Jamie Susskind:

So I can't speak from their negotiating perspective, and that's a thing I would defer to Tim and the Cruz folks and I guess the Cantwells on. I would say, right, two things. One, the issue that I've actually heard a lot more about than PRA right now is preemption. As Tim said, we've got like 10-ish depending on how you define the scope of these bill states. They don't all look the same. I mean, California is a particular agitator and they will come and they have come, and they sort of cry foul about, "What are you doing? And the federal government cannot take away our authority, and our agency is working. And what are you going to do to help us sort of keep going?"

Preemption is tricky. I won't get into tons of details, but preemption has been conversations that we've talked through, both in sort of the COSO context and they've talked about it in COPPA last year. When folks were looking at comprehensive again, it came up. And I don't have a great solution, I mean, right? As Tim mentioned, I think, that I liked what Attorney General Weiser said where he's like, "Well, you want to preempt us? Go right ahead. Give us a strong law and go for it." I've been having sort of off the record conversations with different AGs' offices, just to get a sense of, "Okay, what do you guys see the scope being in each case? If you're comfortable with preemption, where? Where do you draw your line?" And everybody's different. The other thing I would say that Tim did allude to a little bit is that there are members, particularly on the Republican side now, and maybe it's more of the populous members who, for the companies in this room, they want to sue you.

The topic came up during the content moderation panel and I heard people kind of chuckling about it, but for real, they do want to sue you over various things. And I don't know that that's a thing that can just be easily dismissed outright. You can argue about the validity of the 230 stuff, and I'm glad I'm not on that panel. You can argue about whether a private right of action is valid for some of these things against kids. We didn't put it in COSO. We made a concerted effort not to. We just didn't think it was the approach at the time. But that's there and that's not really going away. So there are Republicans that are getting more comfortable with it, because they feel very unhappy with sort of where these tech companies are going.

Shane:

So to broaden this-

Tim Kurth:

Can I just say one thing on that?

Shane:

Sure.

Tim Kurth:

Because I think it's important what Jamie brought up about the preemption and I should have. In my mind it's always clear, but not to everybody that's listening to me. That was like the trade-off for Chairwoman Rogers, is that it's like if we're going to accept this kind of exposure, the same point, this is going to be a federal preemptive law. There's not going to be a question of all these

different, it's not going to be a gotcha equation. We want it to work for all the different stakeholders, so.

Shane:

Great, thanks for that. So part of this, and I'm just going to open this up a little wider, is the challenge of where the data flows. So we have a couple things coming up this fall that have caused some bones of contention, which is the Foreign Intelligence Services Act or FISA, which is known as 702. Schrems, a gentleman from Austria has knocked down our Trans-Atlantic privacy bridge, the privacy shield, and now we have a privacy framework that the Department of Commerce worked very diligently and hard to put in place. So we could have a good symmetry of data flow between the United States and EU, but obviously we need to do this globally. And so I always feel like where we lose control candidly is not, I feel like Meta has taken the brunt of all this with Schrems, right?

Schrems not really that pissed at Facebook/Meta when he started with this. He's pissed at the NSA, I mean more or less. But then you go to the second ring out and it is data brokers and all the data scraping that is going on in, especially now that we have AI and we've talked a lot about this during the conferences, you need a match match win on this. So we're better off having a better concept of how we're gathering data and using data. And some of it, to Kristian's point, you also should just trash it. It's expensive to hold onto. It's a cybersecurity risk because it becomes a data breach possibility, and it's really not that interesting at the end of the day, for people who actually want to monetize it.

So how do we get better positioned, looking at the stuff that Jeff did that said, "People candidly don't really care where their data is located." Some people have been fooled into thinking that if I say, "I have to data localize, I'm going to get a bunch of jobs in my country," and really you're going to get a server farm and a guy who comes in and flips a switch off and on. So, where should we be headed as we look positively on the horizon, knowing that data is very important? We're not quite where we want to be. It looks like Congress is trying to get us better positioned internationally. So what would you say is our next best step going into 2024? Kristian, I'll start with you.

Kristian Stout:

Well, I mean frankly, I advocate for realpolitik as much as possible. I think that, so with the data flows conversation, there's a couple of components here that we're just not ignoring the reality of them, I think. One, okay, so first I'll say, I do wish that we could reform our national security laws because I don't like being spied on too. So I'm sympathetic to that point. But the problem is that every country spies on all of their citizens and everyone else's citizens all the time. So we're in this sort of naive position where we believe that, because the United States happened to get exposed through ...

Shane:

Don't you wish there was also an element where they'd be like, "Your lights are on." I mean, they know all this stuff about you? Like, "By the way, you're in this restaurant and your battery is going to die because you left your car lights on. We know that about you."

Kristian Stout:

Yeah. And there's a level at which the European Union is operating, at which they're pretending that they don't have member states that do the exact same things we do. That they don't have other trading partners that do the same things we do. And I get it. I don't like that behavior

either. I don't like what my government does. I don't like what anybody's government does, but they do it. And if we use that as a pretext for putting up trade barriers, I think that hurts all of us and it hurts the countries that should be allies. So that's obviously your problem.

The other thing is, I don't think, and I always felt like I was screaming into the void for the last few years, is I've been trying to write on the data localization issues. Everybody talks about Meta because they're the ones that keep getting sued, unfortunately. But this is not-

Shane:

And huge fines. Huge fines.

Kristian Stout:

Huge fines that I think are unjustified and hopefully they're getting challenged. But this is not about Meta, this is not about social media or search engines. The digitally connected economy is basically any device that has data, that it can transfer it around on a network, which is like everything now. So we start with Meta as being the problem. And this gets to the realpolitik point. Everybody's doing this, all these governments are doing what we do, and everything we use is connected to data. Which means that if you follow the logic of what the DPAs in the EU are doing and follow the logic of the Schrems suits, you're basically going to shut down a huge chunk of actual trade, not just digital trade.

And this is something that everybody needs to take seriously. And at some point. We need to step back and be like, "You know what? Maybe." We don't actually know what the value of data is. The GDPR is not working out the way we think it is. The PRA will be a tragedy if it comes into effect. All of these, we don't know what we're protecting when we pretend we're protecting privacy, because of the privacy paradox that people have. So what are we even doing here? Why don't we be more realistic with our policies?

Shane:

Sorry, I was just being told to pay more attention to what's on the screen. And there's the question in the audience. So I was looking, I was paying attention to what you're saying. But before I get to all those, because I haven't read them yet, since you are doing all of this work and you have a bunch of policymakers in the room, what do you wish that they would pay attention to first out of, if you could grab one page or one chart out of all the stuff you've done that you think might make an impact?

Jeffrey Prince:

I won't kid myself, but I'll try.

Shane:

Oh, just live in a great world for a moment.

Jeffrey Prince:

Yeah, I guess there's a couple things. There's generally the results we have that I think in a lot of ways speak for themselves. I mean, we focused a lot on the, how much people actually care about data localization. So I do think our research speaks to political motivations based on that idea, which doesn't seem to have a lot of empirical basis. The other thing that I guess comes to mind for me that I just was thinking about as I was hearing the other panelists speak is, I don't hear a lot, I think implicit in all of this conversation, is this notion of legal externalities. It kind of

brings me back to Matt's talk yesterday. In a lot of cases, as an economist, this is often one of the elephants in the room. Is like there's externalities here that are difficult to deal with, but really matter.

And I think in this particular instance, what I'm talking about is the economics of the situation. As I've seen in these applications and in others, completely divorced from some of these localization laws, is this notion that one entity's legal framework or legal decisions or policy decisions make it such that the company that's being regulated, that operates in a whole bunch of markets from a cost standpoint, it's better for them to just then accommodate that regulation or law everywhere. And then voila, you've got a legal externality.

So then if the economics are such that the regulations in one place by one entity, basically cause it to be cost prohibitive for the company to just kind of carve that out and only accommodate that, but then behave otherwise how they were elsewhere, all of a sudden now you've got a situation where it does behoove us to think about in America, we've got this potential benefits from having statewide laws and we can all learn from each other from statewide laws. But as we're seeing with California, California puts data policy laws in place and inevitably it's going to affect the entire country. And why? Because of the economics of the companies trying to accommodate those laws. And I think, that needs to be taken into consideration both within the United States and internationally as we're thinking about, what is a reasonable way to approach this. So that's my two cents.

Shane:

Great. Okay. So I know we're running late, so I have two things. Maddie, where are you? Okay, Maddie, you get to ask the first question. So Jeff, this is one of your students. Maddie will get a microphone, kick us off. I hope you have a question in mind because Scott just told me that you have to ask the first question.

Maddie:

I don't have one yet.

Shane:

You don't have one yet? Does somebody else have a question that Maddie can think? All right. Up here, right in front. She will be paying much more attention in class, by the way.

Maria Scotto:

Thanks, Maddie. Hi. Maria Scotto with Access Now. I just had a quick question. So we know that the EU's AI Act, it's under negotiation and it does provide an excellent case study of how AI legislation is meant to build upon preexisting data protection regulation, how a national data protection law could be critical for effective AI accountability. So it can provide those, a clear and consistent legal framework for data collection, storage and sale. So I think my question might be geared toward Tim and Jamie a little bit. So just in your opinion, do you think that before considering specific legislation focused on AI systems, do you think that the US should have a data protection regulation to ensure that those companies and the data specifically fueling their AI systems, respects our democratic values, and we ensure that it's used safely in responsibility?

Jamie Susskind:

I feel like that's pretty easy. So yes, I think so. And so, folks will come and they'll talk to us about the EU's AI Act, and it's like, "Yeah, that's interesting, but this isn't apples to apples," is what I attempt to tell them. And it's like, look. In the EU, they're building on a whole sort of framework that they've had in place for years. And yeah, there's a lot of problems with GDPR. I wouldn't advocate that we have that in the US, but we need something. And if you're sort of expanding into these new tech areas, particularly with generative AI, it is jumping the gun, I think for us to go forward with sort of a comprehensive regulatory scheme for AI that doesn't take this into account.

Shane:

Anyone else want to add to that?

Tim Kurth:

Yeah, absolutely. I mean, collection, transfer, storage, I mean it's fundamental. We definitely have to have something like that in place before we're speculating on other forms of how AI should be regulated. And honestly, I always worry whatever comes out of the EU, I will EU bash a little bit, because there is the level of protectionism that comes through. We did a bipartisan staff del a couple of years ago and it was interesting, because when you go to the EU, they talk about GDPR as being an export. I mean, that's kind of scary. I don't think of a regulation as export. I mean, I went to a business school, so it's kind of different for me, but so.

Shane:

Kristian?

Kristian Stout:

I actually think the AI Act and the idea of AI regulation bears an interesting analogy to privacy. We don't know what we mean when we say privacy, or when we say AI. AI is a marketing term. We have had pieces of AI technology in our systems for 25 years at this point, that used to be not as good, but now we have it better. AI, when people say AI, it's something that they're trying to get investors interested in their startup. And then politicians happen to notice because they got freaked out when they saw that you could cheat on exams with ChatGPT, and they're like, "Oh no, we better write a regulation about this."

And what the EU is doing, it's very similar to what they did with GDPR. Privacy is a very ill-defined term. It doesn't mean something. It doesn't mean the same thing in every single context. Me thinking, maybe it's creepy when Facebook tracks me and knows that I'm interested in buying a new bandsaw, is not the same thing as when a cell phone company sells geolocation data to bounty hunters. But we call that privacy harms. We don't define the harms. And then we write legislation that gives a lot of power to regulators, to go out and pick and choose what they want to treat as harms.

And we're at risk of doing the same thing with AI. That's fundamentally, the approach the EU is taking with the AI Act. If you read it, it's creating this discretion in the hands of certifying bodies and in implementing bodies to go out and say, "Okay, well what's AI? All right, let's imagine all of the bad things that Terminator could do to us one day, and now let's go in and make a licensing regime to make sure the Skynet never rises." It's not a good activity. What you need to do is you need to go out, same thing in privacy and in AI. You need to go out and actually find where there are actual harms. And then more importantly, where existing laws and regulations don't cover

those harms. Because a lot of times, what we're afraid of are already covered by existing laws, and we're just adding more layers of regulation and law on top of that. So, that's my rant.

Shane:

Jeff, do you have anything you want to add?

Jeffrey Prince:

I'll just be very brief. Legal scholarship is not my comparative advantage up here, but I just wanted to highlight something Tim said, because I do think it's very interesting, because it dovetails exactly that I just said before. Which is, GDPR being an export from Europe to the United States is exactly consistent with the externalities I was just talking about, right? So it's not only I think, highlighting that such an externality exists, but that the enacting entity may be specifically taking that into account in their decision process to enact that law. And I just think that's really interesting, and I think that needs to be part of the conversation.

Shane:

So Maddie, you were just saved by the president of the organization, who told me I had to stop right now.

Maddie:

Oh, okay.

Shane:

So I apologize. We are wanting to get you guys a little bit back on schedule. Thank you for this amazing panel, you gave us a lot to talk about. So give them a round of applause.