
# Reawakening Digital Trade: Diverse Stakeholder Considerations Around The Future of the US-EU Data Privacy Framework

## October 6, 2022 - American University, Washington, DC

**Christian Dawson:** My name is Christian Dawson and I'm Executive Director of the Internet Infrastructure Coalition. We're a trade association of the companies that make up the Internet's infrastructure, particularly the ones that sit above the telecommunications layer but below the content layer, the people that make up what I call the nuts and bolts of the Internet, and we are here today with our partners at our sister organization in Europe called eco, the Association of the Internet, and I am one of your two hosts for the day. The other here is my colleague Oliver Süme, who is chairman of the Board of eco, he is also industry and partner at Fieldfisher.

Fieldfisher is our fiscal sponsor for this event. For those of you who are in the room with us here today, you'll see that we are thanking Fieldfisher as our sponsor here. We also have two other groups I would like to very quickly thank, one is the Inclusive Tech Policy Group here at American University, where we're here hosting today's conversation, so thank you very much to American University for hosting us today in the Inclusive Tech policy group. In addition, thanks to our friends at ISOC DC, the Internet Society Washington DC. today's event is called Reawakening Digital Trade Diverse Stakeholder Considerations Around the Future of the US-EU Data Privacy Framework, which is the forthcoming framework that will finally replace the long now defunct Privacy Shield.

And this is something that I believe is relatively timely. Those of you who are following this issue in the news, and who paid close attention to what's happening on issues of digital trade, know that there are lots of press reports that this new framework is being released soon.

I will not purposefully link that to a note that, if you take a look at the listed speakers for our event, one of them was supposed to be Alex Greenstein, Director of Privacy Shield, who was the lead negotiator from the US side from the US Department of Commerce. Alex had to drop out of being a part of our event here at the last minute. I don't know that we necessarily want to read into that with regards to the timeliness of the conversation that we are having today, but I will note that we are sorry to not have Alex here, but we have a number of wonderful panelists here for a very exciting conversation.

And so, I'd like to go through the panelists that are here today to have a conversation with us about our feelings around the forthcoming US-EU data privacy framework, what we'd like to see, what we believe is important. I'll start at the end, we're happy to have, Catherine Stihler, who is the CEO of Creative Commons. Catherine, I'm very excited for you to be able to give us a little bit of a civil society perspective. And also, Catherine is a former Member of Parliament in the EU, so you have a little bit of a perspective to bring to us there from that perspective. Excited for that. David Snead is my co-founder here at the Internet Infrastructure Coalition. He is also General Counsel at cPanel, so thank you for being here, David. We have Kate Charlet, who's the director of Data Governance at Google, and Alissa Starzak, who's the Vice President and Global Head of Public Policy for CloudFlare. Thank you both for being here today. I've already mentioned my colleague here who is my co-host for the event, Oliver Süme, who's Chair of the Board of eco, and industry partner at Fieldfisher.

And, finally, I've got Ruth Berry. Ruth Berry is Acting Deputy Assistant Secretary for International Information and Communications Policy at the Bureau of Cyberspace and Digital Policy at the US Department of State. Does that all fit into business card?

**Ruth Berry:** Barely.

**Christian Dawson:** My hope is that we can start this conversation by asking you, Ruth, to give us a little bit of a level set on what it is we know today around what, can be expected, hopefully soon, about the US-EU data privacy framework, so that the rest of these experts can have an as informed as possible discussion, with you and with us, about what we are going to be hearing in the coming days.

**Ruth Berry:** Sure, great. Thank you. Really glad to be here. Thanks for inviting me, Christian, and really glad to be with all of these panelists here today. So, as you are all very likely well aware, the US President and the Commission President von der Leyen announced a deal in principle on a new Transatlantic Data Privacy Framework. This was something that had been heavily negotiated, which I was very involved in at the time

from the White House over the past year and a half. And so, we were very pleased to be able to get to that place in March.

Since then, the United States has been working to translate that deal in principle into legal language that would be released in the form of an Executive Order and Department of Justice regulations. We believe that this deal addresses the deficiencies and the shortcomings of the previous Privacy Shield Framework, that were outlined by the European Court of Justice in the Schrems II decision, and will provide a durable basis for transatlantic data flows that really are critical in the lifeblood to underpinning the $7.1 trillion transatlantic economy.

The new Transatlantic Data Privacy Framework puts in place rigorous protections regarding the necessity and proportionality of signals intelligence collection, and creates a multilayered, binding, and independent redress mechanism for those who feel that their data has been improperly accessed by US intelligence or law enforcement.

And, that two layer includes a review by the Civil Liberties and Protection Officer at the Office of Director of National Intelligence, followed by an appeal mechanism through a new data protection review court that will be housed out of the Department of Justice. And so we are, as I said, very pleased to be putting this framework into force, in the very near future.

And I think there'll be a lot more details on what that looks like in the coming, um, near...

But, of course, I come from the State Department, and so I would like to talk a little bit about what this deal means, and how the Department of State and this administration is approaching data flows from a geopolitical standpoint, because it's an incredibly important issue.

And so, I think, first I'll just provide a very brief overview about how the Department of State has arranged itself. So, as he mentioned, I come from the new Bureau of Cyberspace and Digital Policy, which was stood up in April as part of Secretary Blinken's modernization agenda, and this bureau brings into one sort of unit work on international security and cyberspace, work on international communications, information policy, digital economy, as well as a brand new digital freedom unit within the bureau, and this really enables the department to both integrate the national security, human rights and economic issues when it comes to digital and emerging technologies, as well as elevate these issues both in terms of the State Department's role within the US interagency, but also in terms of our international diplomacy.

And, one of the key issues is data policy and data privacy, data governance, data sovereignty. These are all issues that you hear a lot in the international debates, and we think that this is a key geopolitical issue and an area where you can really see technology competition playing out. And Secretary Blinken has said that he sees our

task is to put forward and carry out a compelling vision for how to use technology in a way that serves our people, protects our interests, and upholds our democratic values, and data policy and data privacy are central to this.

And, we seek to work with a community of like-minded democracies in developing shared approaches to these challenges, that reflect a strong commitment to privacy protections while simultaneously allowing cross-border data flows that open market led economies and societies depend on, and this new data privacy framework represents that commitment.

And, I think, having the US and Europe together on these issues really creates opportunities for us to turn globally and think about how we're working to help build a 21st century future that embodies these principles and democratic principles.

And so, while I know a lot of discussion today will be on the data privacy framework, and I'm happy to discuss it in as much detail as I am able, I just want to hit on two other really important efforts in this space, and one is our work with our partners and allies at the OECD to develop shared high level principles on trusted government access to data held by the private sector, and we're hopeful that there will be significant progress on that effort in the coming months, and that includes partners from Europe, but also from other OECD members such as Japan and other democracies.

And then, when it comes to commercial data privacy principles, another effort that we're working on, that Commerce is very involved in, is the globalization of the cross border data privacy rules systems, which we anticipate will soon be open to participation from jurisdictions around the world, and something that we're really encouraging organizations, companies, and countries to sign onto, because it can demonstrate that economies can come together and respect privacy and democratic principles, while still fostering economic openness in a way that's interoperable. And so, it's not just about, Is privacy being protected? But also, countries are able to figure out how to do that, and companies, within their domestic government and political systems.

And so, it creates much more interoperability, which I think is really critical as we think about expanding global data flows and protecting the free flows of data.

So, I will pause there, because I know there's a lot of other great speakers with things to say on these topics, but just to say that this is a really exciting area and one is that the forefront of our priorities at the Department of State and the US government.

**Christian Dawson:** Ruth, I want to thank you much for providing us that context going into our expert panel discussion. I'm going to throw it to the panel for reactions to what it is you've said in just a moment, acknowledging the note that you said about being only being able to answer what you can. We can't press you on things like, when's the EO coming out, we'll have to respect that. But, before I throw it to the panel, I wanted to also thank you for taking the time to come and provide that information, on what is, I

know, between the work that's being done on this, and the work that you've been doing in and around the ITU, including just getting back from Romania, Bucharest?.

**Ruth Berry:** That's right.

**Christian Dawson:** ...and the ITU, you must be very tired. And the fact that you take the time to do that's really appreciated.

**Ruth Berry:** Thank you.

**Christian Dawson:** One quick note about that. Internet governance is one of the issues that i2Coalition, our organization, and eco also work closely on, and we were very excited at the work that the US government did towards the election of Doreen Bogdan-Martin at the ITU, which I think was accomplished last week. We are here at American University being hosted by them today, I will note that Doreen Bogdan-Martin is an alum, so we give a great celebratory thanks to you and to Doreen for having moved that forward.

**Ruth Berry:** Thank you. Yeah, we're very pleased with her success in the campaign for Secretary General, and she really is incredibly qualified as a 25 year veteran of the issue set, and within the ITU, and the first woman to serve as the Secretary General of the ITU in its 157 year history, so we're very pleased for her success.

**Christian Dawson:** Wonderful. And so, my last comment before I throw to the panel to start reacting to what will be discussed here today, is to say that, along with Internet governance, digital transatlantic data flows is one of the main issues that i2Coalition and eco, our partner organization, work very closely on, and it is because, for the businesses that both of us represent, this type of ability to transact across borders is extremely important, so understanding that, we believe that the issue itself is extremely important. I would love to know from our panel, how extremely important, is this EU-US Data Privacy Framework that we're looking at, particularly if it is, and I centered on one word that you said, durable..

We have a mic here and so anybody has any thoughts to share? Grab the mic.

**Kate Charlet:** I'm Kate Charlet from Google, for those who are dialing in. So, I think, just on first principles, people want to be able to access digital services from anywhere in the world, and they want to know that is private and that their information is safe and protected, so really commend the US government and the European Commission on all the work that they undertook to get to the agreement in principle, and now, obviously, all the work that you've done to get to this point of being able to release the Executive Order soon. I think it's clear that all of that work was anything but trivial, and I appreciate very much the approach and the time to ensure that agreement is a reliable agreement, a durable agreement, and a foundation for future data flows, and I think

that commitment is clear, on all sides, to a high standard of data protection from this process.

As Google, we've long advocated for reasonable limits on government surveillance, and it's an issue that requires greater trust between governments, and that's why, hearing you talk about the OECD process, and of the geopolitical trust building that is part of that OECD process around government access to data, is really important to that question of stability.

And, it's really welcome to hear the US committing to enable independent and meaningful redress for people in the EU, to strengthen the guardrails and proportionality around US Intelligence collection, and to ensure effective oversight over these new privacy and civil liberties standards, so, it seems, in ways that really are responsive to the concerns that are raised by the court and the European Union, and this is the kind of thing that citizens expect from democratically elected governments, and, so we're really looking forward to the next steps in the process, and look forward through this process to conversation talking about CBPR, as well, in OECD, because I think all of those are multilayer initiatives that, even beyond this immediate moment around the Executive Order, and the process that will play out over time following its release, there's a number of initiatives that we need to layer on, when we're truly thinking about long term stability, interoperability, scalable protections for data flows.

**David Snead:** I'll follow up to that, and thank you for all the work that you've done. I know that it's been a lot of extreme heavy lifting, and it's not unrecognized. I'm David Snead, and cPanel is a piece of software that, along with our colleagues in Germany and Switzerland who run Plesk, really facilitates small businesses. Our customers are mom and pops who run grocery stores and things like that, so this is a very key regulatory issue for us.

I was wondering if you could talk a little bit more about durability, that's going to be a very interesting topic for us to understand when we're planning on whether we're going to incorporate this new process into our contracting processes, and things like that.

**Catherine Stihler:** Thanks so much, Ruth, for that. I thought that overview was fantastic, and I think that the fact that we are seeing the two countries, the EU and the US, actually come together to really address the citizen's perspective over privacy, which is where this all came from.

I was curious to know whether the proposed redress mechanism will actually also involve the supervisor, say, in the EU? How will that work in practice? Because I've worked on redress, when I was in the internal market committee as vice chair all those years back, and now I've got two hats from Creative Commons as a CEO, and also with my previous experience, so I'm curious to know how you see that work in practice. Clearly the devil will be in the detail, and it'll be, how water tight it can be in terms of whether there will be another challenge in the future, we can't predict that.

But, I think the fact that, for the EU, for years this has been a real friction, as well as a problem that had to find a solution, even though the problem was something that we all agree, that privacy's important. So, I'm just really curious to think a little bit about that, because clearly, from a citizen's perspective, the redress stuff has to be clear, it has to be succinct, it has to be accessible, and also perhaps has to make sure that, clearly from the EU perspective, it has to be in 23 different languages, too.

**Alissa Starzak:** May I take advantage of the fact that the microphone is here, too, with a follow up question, and I agree, thank you so much for all your work on this, it's so incredibly important from a US business standpoint, but just the ability to have some certainty. We've all sort of highlighted the durability component, that's an incredibly important thing.

I should have actually added, I'm Alissa Starzak from CloudFlare.

The question I wanted to ask was somewhat related to that, not entirely on the redress side, but actually on longer term sort of statutory changes. So, following up on Kate's question as well, I'm curious how the US government is thinking about those questions, if that is also part of the longer term picture, even if it's not in this immediate potential action?

**Ruth Berry:** Thank you. I'll try to hit the questions that were raised, but please, if I miss anything, remind me. As I said, the deal that was announced in March, as a deal in principle, was not sort of a theoretical agreement to come to an agreement, it was based on incredibly detailed 18 months of negotiation between all the important lawyers in the US government, and the incredibly indefatigable and motivated and smart lawyers in DG Justice on the European Commission side in the Commission legal service, so I can say that this was a very legal discussion, looking very closely at EU law, US law, the Schrems II decision, and what's possible within that. And so, unfortunately, while I can't get into additional details on the exact mechanisms of the redress, I can say that anything that we agree to is something that both our lawyers and the commission's lawyers believe addresses the Court of Justice's concerns, and will stand up and be a durable solution.

I can say that nobody, on either side of the Atlantic, who was involved in these negotiations, wants to see another agreement overturned, and so that was certainly a shared motivation throughout the entire course of these negotiations, and as we work to translate this agreement or deal into legal text.

I think there will be future legal challenge, I think that is one thing we can be certain of, but another thing that I would say, and I think this has really been highlighted by the work in the OECD, is that the way the United States approaches government access to data held by the private sector has a lot more in common with our European counterparts than it does different. And so, when we think about the durability of the solution, we also have to look at what are European member states doing, and,

particularly with the reforms that are being put in place, we are in good company among our European allies, and that hopefully also would put us on firm footing when it comes to how the Court of Justice reviews these.

So, this deal is done with executive branch authority through an Executive Order, and the authority of the Attorney General to issue binding interpretation of US law, and so we believe that through executive authority that we are able to put in place what is needed. I also think, based on, sort of, our constitution, and system of government thinking through where the authority rests when it comes to national security, that is something that is vested within the executive branch, and so it's unclear that legislation could serve the purpose. So, that being said, this deal's based on executive authorities and action.

That being said, in the future, I know there are conversations about federal privacy legislation. The White House recently released a Tech Accountability Agenda fact sheet, and called on Congress to pass comprehensive federal privacy legislation, which is more likely to focus on how US companies handle data, but I think is something that would absolutely help bolster the conversation about US companies and how they protect privacy.

So, I wouldn't foreclose future legislation in this space, as for the buttressing or bolstering this deal, but we believe that the durable framework can be created without legislation.

**Christian Dawson:** Thank you for taking the questions. David, you mentioned that your company is interested in this, because the small businesses that you represent, that they need this, and we are talking about this because we believe that it's important for the businesses that we represent and their customers. So, I guess, my question is, obviously we have not seen the language that we are talking about, so with that one big caveat and asterisk, the idea of this Data Privacy Framework, is it something that we expect is going to stimulate transatlantic business?

And I've got a specific question about diverse businesses, big and small, is it going to be able to stimulate the economy in those areas on both sides of the Atlantic?

**Oliver J. Süme:** So, I'm absolutely convinced it will be able not only to stimulate, but to do something more important. and that is to end the huge legal uncertainty that a European business, and in particular the small and medium sized companies, are currently facing, that's the biggest burden currently, and, as many of you will probably know, the Privacy Shield was the most important legal ground for international data transfer, in particular for small and medium size companies.

The huge multinationals, they can rely on other legal grounds. Some of them have binding corporate rules, implemented as a legal ground. As many of you know, many companies are working with a standard contractual clause, but that's already something

that is pretty challenging for a company to implement it in a proper and compliant way. So, the big advantage of the Privacy Shield, and I hope of the new framework as well, is it's easy to handle. You just needed, under the old Privacy Shield, to register, and it was very easy and comfortable, and again, in particular, for medium size companies to rely on a very stable and easy legal ground under the GDPR for international data transfer, that's what I do hope will be again the case in the future.

And then, I'm sure it will not only stop the situation of legal uncertainty, but, as you said, will stimulate data transfer and a global data economy on both sides of the Atlantic.

**Alissa Starzak:** I definitely agree with that. I think the other thing I would say that I really liked in your comments, is the idea of shared vision of privacy, because I think some of the things that we face in the EU, it's the legal uncertainty, but it's also the sort of perception problem from a company standpoint, the sense that the US and the EU are not aligned on privacy, and so, to the extent that is part of the work that you've done, we really appreciate that. It certainly improves long term help for US companies, and particularly small and medium as well, it enables cross border work.

I agree as well, that anytime you've got uncertainty behind trillions of dollars of trade, it's going to help to have a resolution to some of these questions, but I also want to point out that this isn't just about business and transatlantic economy, data flows are good for cybersecurity, data flows are good for resilience. There's a lot of reasons for us to do this work, to bring those protections that are necessary, and lead to broader stability.

**David Snead:** So, just going down, I'll echo what Oliver said, but the other thing that I'll add is, having something that is easily usable, and easily implementable, actually helps consumers, because, let's be honest, most small businesses right now, they're not doing anything to comply with GDPR, right? And so, if you put something in that facilitates compliance, it actually helps consumers on both sides of the Atlantic ensure that their privacy is protected, so that's one of the reasons that I'm kind of excited about this actually getting across the finish line.

I guess as well that, at the moment in the EU, there's the whole debate that's happening on new data rules, not that this will affect what will come after the Privacy Shield, the new framework, but it's interesting and curious to see. The way it's being debated at the moment is very much in line with what you're describing about where things in the discussion are going in the OECD, and about how the value of data is better exchanged. There's something which is going to add real value, and they've got a very short window, because the European Parliament elections are in 2024, and so, if you want to get anything through, this has to happen this side of the election.

**Catherine Stihler:** So, I'm just very curious, Ruth, if you've been thinking a little bit about the new data rules, just in general? They're very in line with what you're describing about the discussions at OECD, I'm just curious to know thoughts and views?

I think, the Transatlantic Data Privacy Framework solves a very real problem of legal uncertainty around transatlantic data flows, but, of course, it fits within this broader policy and geopolitical context that I mentioned that governments are grappling with around the world in terms of, what does it mean to protect privacy and protect data? What does it mean to ensure free flows of data? I think this common thread of data free flows with trust, that's come up in the G7 quite a bit, and has sort of tasked the OECD with some economic analyses around data flows, so, I think it's really important conversation.

**Ruth Berry:** I'll talk briefly about the US-EU Trade and Technology Council, which is a forum for a lot of conversations between the US and Europe around technology issues, and while data privacy is not discussed explicitly within that context, there are a number of things related to, and I'll say Working Group 5, thinking through regulatory approaches when it comes to platform governance and data governance, and so I think there's a lot of conversations. Of course, the European Union and Commission does not negotiate its legislation with the United States, in the TTC or any other context, just as we would not, but it does offer a forum for us to have really open discussions about thinking through, if we have shared values and objectives, how do we ensure that the regulations that are being put in place, at least align, and do not overreach and go too far in terms of stifling innovation, or backfiring, or, frankly, being too complicated to even be implemented.

I will say, I was recently in Brussels, and Paris, and had a lot of conversations about a number of pieces of EU legislation coming through, whether it's the AI Act, the Data Act, DMA or DSA implementation, or thinking through discussions around an EU cybersecurity certification that could potentially have domestic ownership requirements. So, there's a whole lot of areas where I think having this issue settled in terms of equivalency of law, when it comes to protections, I think will help create a little stability, and feed in to the other conversations that are happening around digital regulatory issues.

**Christian Dawson:** Thank you. I'm going to jump in with another question, we've spent a little bit of time talking about how it's very important for businesses to have more certainty, but I'm interested in changes from a consumer and data subject perspective, I'm interested in finding out more about their certainty. Will changes in the way that data's shared between countries, particularly data to the US, from the perspective of the panel, and I'm very interested, Catherine, in hearing your perspective on this from a civil society perspective, do we expect this to add comfort and trust to the general Internet?

**Catherine Stihler:** As for all Internet users, I feel like I'm on the spot. So, again, the devil is in the detail, right? I do think that there's a different debate around privacy today than there was so many years ago, and just a different environment that we're existing in. There's also different questions at the moment around how we want to see the Internet that we want, in terms of what does good look like, we know what bad looks like, but

what does good look like? That's a bigger conversation than just the framework that we're dealing with data.

But, from a consumer perspective, the strength that the privacy issues have been dealt with, and taken very seriously, had to because of the court ruling, but also two years on, that you just described, Ruth, lawyers talking to lawyers, I mean, that took 18 months, it takes time, right? But, if what comes out of that is a strong, legally certain document that we can all agree with, then that has to be a good thing.

You're right that there may well be a challenge, and it will be picked apart, but the fact that the goodwill that's there between both the Commission and the President is just, very helpful, and I think that that goodwill is taken very seriously. So, I'm really excited about what will come out, and hopefully it will add to that, the advantage we all want to see, but again, the devil's in the details, so I look forward to seeing what is there.

**Kate Charlet:** I'll just say to your point about trust, trust has been part of this conversation, really an integral part of this conversation on data flows. really probably dating back a while, but really to when Japan had their host year for the G20,the term 'data free flows with trust' was coined, and, I think, since that you've seen the G7, you've seen the OECD and others, kind of pick up this notion of trusted data flows, and I think that's a good thing. What is increasingly clear, though, is trust has to happen on many levels, and it has many layers to it. It's trust between users and service providers, it's trust between service providers who are sharing information with one another, and really what was very prominent in this conversation around US-EU data flows is there has to be that geopolitical level trust between the countries where data is flowing. At its heart, this was a case about not company practices, but that geopolitical level trust, and we have to think about it on all of those layers.

I also think, even when we're beyond kind of this direct question of US and EU, Ruth, to your point about the global CBPRs, we have to find globally scalable models and interoperable models to build that trust on a broader global level. That's why we've been very supportive as Google of the work on the global cross border privacy rules. We are looking to certify to that when we are able, and work with the community too, to really think through that process, and think about what it takes to bring that trust to a broader scalable level.

I fully agree with all of it, not surprising. Actually on that trust piece, I think one of the challenges that we've seen is that those breakdowns in trust then have profound follow on effects, and so you end up with the question about whether people trust their own governments to negotiate, and then people, of course, have the agreement within governments.

**Alissa Starzak:** And, I think, we have seen that, over the past few years in the EU, in pretty profound ways, where he legal frameworks themselves, whether those are adequate or not. The lack of trust then erodes business, from a practical standpoint,

because people are concerned about how their data might be used, and they don't feel like even the existing frameworks work, and so thinking about the durable frameworks that are global certainly is a really important step long term. I also want to go back to something that, that Kate flagged. The other component of that that becomes really important is thinking about the reality of the importance of data flows, and emphasizing, when you start getting into the world of data sovereignty in particular, and some of the other bills that you're talking about, that there are a lot of areas where the kinds of data that might be shared, it's actually remarkably helpful for normal citizens to share that data for long term goals that are in their own interest, and yet, we don't always have that more nuanced conversation about the data sets that actually make sense to share, and what that looks like, and we're not even talking about personal data when we start getting into the data questions, right? So, thinking long term about how to tell those stories and explain to people on the ground about what the long term goals are, I think, is a really important step.

**Ruth Berry:** I just want to follow up a little bit on this idea of trust, and I think you listed some sort of relationships of trust and you sort of hit on another one, which is absolutely citizens and governments, and government access to personal data, which is often held by the private sector, right?

I think there's both the geopolitical aspect, but also just, in Europe in particular, the idea of privacy is very important to European citizens, and as they think about that, what's important is that we are better able to draw the line and make clear that there is not a legal or moral equivalence between how democracies access data and how countries such as the PRC do, and the checks and balances that we have, and I'll be frank, I think that conversation has gotten really lost in Europe, and there's a lot more focus on concerns around US government access to data, at the expense of looking at some actually much more egregious and concerning trends that are happening with authoritarian governments and how they approach this issue. And, these threads are all connected if you look, like efforts to place the Internet under greater government control and take it out of multi-stakeholder governance systems, we see these efforts with the new IP that the PRC is pushing in every fora where it has a chance, and so I think this idea of, really, how can democracies come together and make clear that there are differences and that there is not a moral or legal equivalence, and to do that we have to stop arguing amongst ourselves, and so I think the resolution of this issue between the US and Europe creates a really important opportunity to then take that conversation outward.

And, as I mentioned before, I think the OECD trusted government access to data, by governments for data held by the private sector, does really exactly that, by drawing those clear lines about those differences. So, it really is a global conversation even though it's playing out in many countries, and bilaterally with the US and others.

**David Snead:** I just want to say, yay.

[laughter]

**Catherine Stihler:** Me too, David. But, what I thought was really interesting though, if you think back, was it just last year when I think it was the G7 did the Open Society, why openness and democracies were linked together, and what you're saying about why open data is really important, and sometimes we lose that.

Clearly, that comes with caveats, right? But the importance of how interoperability, how we look at the same standards? We need global rule setting, but how do we do that well? But, we have to start somewhere, don't we? And we have to start with that cooperation with like-minded, not institutions but countries, and nations, and those that have similar values, but I do think it's a huge challenge that we have, that we need that balance with open, to be able to see that link with our democracies, as well.

**Ruth Berry:** I'll say something else too, just because you said that idea about setting the rules and open standards, and I completely agree, but I also think, as part of that, it's incredibly important that we bring in emerging markets and developing countries, because I think this idea that the G7, or advanced industrial economies, set the rules of the road for 21st century development and deployment of technologies or standards, I think it is outdated and comes at our peril, because we need to make sure that the countries that have incredibly growing economies, incredibly growing populations, are centers of innovation, are also able to be part of the conversation about how technologies are developed and deployed, if we want to bring them into that community of open societies, and the trusted network of countries who share the same values when we think about the future of technology.

And so, from where I sit at the Department of State, that's a really big priority in terms of how do we really expand these conversations. Just one example I will give is, we have a program on AI Connect that brings AI practitioners from countries around the world, including a lot of emerging markets, to talk about how do we think about the responsible development and deployment of AI, and creates a community of practice that's not just based in major G7 capitals, and so I think that's something that's really important.

**Christian Dawson:** That's fantastic. We also had mentioned, at the top of our time today, that you'd just gotten back from conversations at the ITU in Bucharest, and I think that some of the conversations that are happening there tied directly to the kinds of things we were talking about today.

So, I think that there is a lot to unpack there, and we were talking about the issues of transatlantic data flows within the framework that happened at this government level, which we could spend our entire time talking about. But, I wanted to take a moment to bring back down to the company level, and to spend a little bit of time talking about a few logistical matters, so that we're talking about the same thing from the perspective of the companies that Oliver's organization and mine represent. One of the

conversations that we had prior to this meeting made me understand that it is expected that previous registrations will still work, and that the old system will, basically, be able to be made retroactive opt in, do you know if that is still the case?

**Ruth Barry**: I have the great fortune of not being with the Department of Commerce who manages the previous Privacy Shield Framework certifications, so all I will say is that the vast majority of the areas of focus were related to government access, and how we think about that, and absolutely the goal is to ensure that companies continue to be able to take advantage of the certification system as easily as possible, but I will refer you to the Department of Commerce on all details.

That sounds good. My other logistical question centers around what Oliver had mentioned around how many organizations, in the absence of a framework, have been relying heavily on contractual clauses, and my understanding is that the use of contractual clauses is something that has been acknowledged and incorporated into the process of the...

**Ruth Berry:** Yep. No, that's a great question. So, the protections that are being put in place, under this Executive Order in Department of Justice regulations, apply to all signals intelligence, and so, therefore, would be applicable to data transfers, whether they incur under some sort of a certification scheme, or standard contractual causes, or binding corporate rules, and so it is intended to provide an important legal basis for a broad range of data transfer mechanisms.

**Oliver J. Süme:** That's great.

**Christian Dawson:** Excellent. Are there any other logistical questions that anybody has about how we can expect this to interoperate with us and our businesses?

**Oliver J. Süme:** So maybe we can, at the end of the discussion, speak a little bit about the timeline for the further process?

**Christian Dawson:** She may not able to comment on it, but yeah, let's speculate away.

**Oliver J. Süme:** Yeah, no, timeline in terms of what happens once we have seen the Executive Order on the European side?

**Christian Dawson:** Oh, why don't you guys do that? That'd be fantastic. Yeah.

**Oliver J. Süme:** Because, it will not be the case that, once we have seen the Executive Order, everything will come into effect, but the European administration will need to take their time as well. They will need to consult with the European Data Protection Board, they will need to consult with the parliament, and then at the end of that process, they will have to publish the whole agreement in their gazette as well. So, that

will add another like three to four months at the minimum, which means, even if we should expect the Executive Order tomorrow, we will see the new framework work only in three or four months at the very earliest point of time, which adds additional time of uncertainty, and it will be very interesting to see how the authorities in Europe are dealing with that. The data protection watchdogs, they need to find a position for this situation as well, and, most importantly, they need to align, so that we do not have different perspectives of this in different European member states, and that's another thing that will be interesting to see how that works.

**Christian Dawson:** As a European lawyer who interfaces with companies to advise them on exactly those types of things, do you have any speculation as to how that'll play out?

**Oliver J. Süme:** Well, I read in a German news magazine, only this morning, that at least some of the German authorities already said that they will be very reluctant in the next month in terms of investigations, and even fines, but that's only what we heard from some of them, and I think it would be very important that not only the German authorities are aligned, but, even more important, or the European authorities find a clear position on how they deal and how they act, or not act, which would be the better option, against companies in the coming months that are just not in the position to comply with the requirements, because an important piece in the puzzle is still missing, so that's very important that we see an aligned voice of the European data protection authorities.

**Christian Dawson:** So, we may end up in a situation where, even once we've seen all the documents, we're in a temporary period of wait and see. Does that seem accurate? And how does that align with everybody's levels of excitement?

**Allissa Starzak:** So, can I ask, and this may be a question you can't answer, but I'm curious actually, going to that piece, do you anticipate that the Executive Order will be immediately operational, or will there be an implementation period on the US side as well?

**Ruth Barry:** What I can say is that the Executive Order will form the basis for the European Commission. I can't get into too many details on this, unfortunately, but I can say that I think the timeline that he laid out is accurate, in terms of the Commission will then have to use this Executive Order to form the basis of adequacy decision, and the question about how DPAs will handle this interim period is a good one and an open one. Of course, we would hope that they would, in light of radical changes to US law being put in place by the Executive Order, they would have some forbearance in terms of how they approach enforcement in this middle period, but that's something that, I think, conversations that will need to be had once the Executive Order is released.

**Christian Dawson:** So, one of the things that I wanted to address within the group, you'll note that the specific organization within the American University that is hosting us today is the Inclusive Tech Policy group, and, the title of our event is Diverse Stakeholder Considerations, and part of that is diversity in perspectives within the panel, but I'm also interested in, once we have a robust and durable framework in place, talking a little bit about how important it is for it to be accessible to all levels of business, and all different data subjects, and part of making it accessible isn't just having an easy signup process, but also ensuring that the language is sufficiently easy to understand and not legalese. I'm wondering, am I right, from the group first, in saying that aspect of it is important, before we see if there's any comments at all that can be made about that?

**David Snead:** So, I'll comment first, saying don't knock legalese, as somebody whose job is to write the contracts that nobody ever reads.

But, I think it's important that it be easy to understand, and that it also be easy to understand from the perspective of the US organizations who might implement it, so I'm thinking like TRUSTe and the Better Business Bureau and the folks who are implementing these things for smaller businesses, I think that that is important.

It's also important, to the extent that it is perceived as a US and EU achievement, for European consumers to actually understand what it says, so they get an idea that it does restrain, to some extent, US surveillance issues, which are a continual problem for the adoption of US technology in Europe, is the perception that US companies are just shoveling information right into our surveillance infrastructure, so something that is easy to understand from the EU perspective would also be helpful.

**Christian Dawson:** That's worth unpacking of itself. Is that the prevailing perception?

**David Snead:** Is that an actual question? Oh my God, yes. We get more questions about how we interact with law enforcement than almost any other privacy questions. We have a webpage that describes our interactions with law enforcement, how law enforcement gets information from us. It's a very critical part, not only of our ensuring that consumers are confident in our software, but also in marketing, and helping folks understand what we do.

**Christian Dawson:** So, this does seem like a real challenge, because it sounds as though it's extremely important that for the robustness, for the durability of it, that the legalese be something that stands the test of both US and EU law, while it being extremely important for a general person to be able to understand it.

**David Snead:** Absolutely, yes..

**Christian Dawson:** That's a very tough bar.

**Kate Charlet:** Yeah, and you have to unpack it. So, the EO and the surveillance changes that are being made need to be explained well. The guidance to US companies that flows from this, or continues previously, needs to be clear and actionable. But, it should be legalese, right? These are legally binding instruments that need to be sufficiently comprehensive and thoughtful, and all of that's going to take scrutiny and review, and so we should embrace the legalese. That doesn't alleviate the need to be out there and talking in very clear terms.

But, I think we should recognize that all the work that has gone into this is to create a legally binding instrument, and that's going to require some level of detail.

**Alissa Starzak:** I think that's right. The other piece that is driving some of those is this sort of skepticism that comes from multiple channels, right? So, if you have skepticism from data protection authorities on the question of whether something is adequate or not,or the surveillance regime, then that then trickles down to consumers, and it drives interest in that exact webpage that has the FAQs.

So, recognizing as Kate said, that you need the legally binding language to satisfy the legal authorities who are looking at exactly that piece, they're hopefully the goal, again with a long term privacy vision that it should trickle down to consumers as well. If there's more trust in the entire system, that should overall, hopefully, help. I would think, because a lot of the questions that we get frankly come from pressure from DPAs on entities, who then want to be risk averse, and don't want to have to answer questions from DPAs in Europe, and that is its own challenge, right? So, they tend to be, It's not the question of whether it's legally appropriate or not, or legally satisfactory or not, they don't want to have questions from DPAs at all, and that is an even more significant problem, I think, from a US business standpoint.

That's not a good result for the smaller companies who have less ability to find options, and it's not a good result for US companies who have a harder time describing what the process looks like.

**Catherine Stihler:** I think you can do both. There's a lot of work that's been done to make sure that legalese is also being able to be in very much plain English, and there's actually an organization that sets out just to achieve that. But also, if you look at a lot of the consumer protection work, particularly that I'm aware of in the EU level, a lot of the work has already been done to think about language, and to think about what you were talking about, redress mechanisms, online dispute resolution work, that's been done to make things very simple and straightforward. There's so much work already been done, you don't need to reinvent the wheel when it comes to some of this.

But also, if you want to bring people in, the question was how do you keep it inclusive? When I think about inclusion, I really think not just about the language and the legalese, I think about someone with a disability. How do we make sure things are accessible?

How do we make sure, say at the EU level, that it's translated into 23 languages, effectively?

And we all know that things can be lost in translation, as I've observed many times. And so, those are some of the other challenges that maybe need to be thought about, but there's been a lot of work, particularly on the consumer protection level, that we can really learn from and take that forward with what we're doing just now.

**David Snead:** So, can I take the conversation in just a little bit of a different direction?

**Christian Dawson:** Sure.

**David Snead:** So, one thing that I wanted to call out that Ruth mentioned, that I think is worth emphasizing, is that this is a bit of an opportunity to show how an open Internet can work, because there are a lot of challenges to an open and interoperable Internet right now, and having the largest industrialized democracies work together to facilitate a continued open Internet is very important, and it's honestly worth celebrating. I know that we're all sitting here with our heads down going, When the hell is this thing going to come out, because I gotta deal with this? But it's worth celebrating, these two groups are working hard to make sure that the Internet is open, and that is worth calling out.

**Christian Dawson:** You gave a yay before. I'm going to give a yay to that one.

**Kate Charlet**: Well said.

**Christian Dawson:** So, we're starting to get close to the time for our conversation today, but we do have a discussion going on in our chat, and I wanted to very quickly call attention to a couple of comments, comments I'm going to reframe as questions, and then, after what's been already talked about in the chat, we'll go ahead and shift to closing comments. So, there's a discussion about concerns that the European Court of Justice will be able to accept anything. There's talk about expecting a Schrems III, and in one of the areas, I guess I'll reframe as a question, is a US law called the Cloud Act seems to be particularly problematic when it comes to the European Court of Justice, taking a look at what they can expect from us companies who are beholden by US law?

My understanding of the Cloud Act in broad strokes would be to treat a European satellite office as US home turf, that anything less than the abolition of the Cloud Act by the US will likely not pass the standards of the European Court of justice, is basically the framework that's presented here.

**Christian Dawson:** Do we have concerns that existing US laws could lead us down the path of a Schrems III decision? Anybody?

**Ruth Barry:** I'll speak briefly to this. Again, not being a lawyer, and not working for the Department of Justice, but my understanding is the Cloud Act actually did not change US law with respect to their ability to issue a warrant for data held by the US private sector, what it did do is create a process whereby foreign governments could serve process on US companies, through a regular rule of law process, for data that they believe is necessary in the pursuit of criminal activities, without going through what is frankly a fairly cumbersome and lengthy MLAT process, which is the current process whereby governments can seek that data by going through the US government.

So, I think that there has been a lot of fundamental misunderstanding of the Cloud Act and what it means and what its implications are, but I would say that this agreement was reached with the Cloud Act being in place, and it reforms being made under the Executive Order regarding signals intelligence, and so we do not believe that sort of the existence of the Cloud Act is something that then would undermine the durability of the Transatlantic Data Privacy Framework that we have worked out with the European Union. For us, when we think about the Cloud Act, I agree with the general framing there, I think the question again goes back to the points you made earlier about the OECD frameworks, thinking about what access to data means in a digital world, where we actually don't store paper at home, right? Where our records are not just stored in a box in the corner, I think the Cloud Act really was designed to address what a future looks like. The challenge in this space is making sure that there is an understanding of that.

**Alissa Starzak:** And again, this is the work across the EU with data privacy, for example, on those questions, which are really about how you modernize questions of access to digital evidence, and that is a long-term goal that needs to happen. I think that, if you explain the Cloud act correctly, what the goal is long term, it sort of makes sense for people, and as long as there are protections in place on government, and just law enforcement access to data, not even surveillance questions.

**Christian Dawson:** I do note that somebody else on the chat put that the Cloud Act was not relevant to the Schrems II judgment, so it was not an aspect of how that one was...

**Alissa Starzak:** It does raise challenges for US companies. One of the reasons those law enforcement questions are so important, though, is because this idea that a US company, and you can't have ownership of a US company, from a provider standpoint, it's really long term problematic, and that's where those questions come up. This idea that anybody who might be subject to the Cloud Act has challenges, that doesn't work, obviously, from a US business standpoint, and, frankly, from a European business either. If you have a European entity with a US office, you are also subject to the Cloud Act.

So, there's a long term challenge of just explanation, and also making sure that people understand their protection sometimes.

**Christian Dawson:** And, David, the page that you were talking about having to put up about, does the Cloud Act play into that?

**David Snead:** It plays into it, it also plays into, to some respects, how we select vendors. There are a lot of concerns from my colleagues who are not in the US about purchasing software and services from US companies, specifically because of the Cloud Act. It does get misinterpreted, but it's still something relevant to talk about.

**Catherine Stihler:** I also think the European data supervisor comes into play as well, not just the court, so we need to also think about that level of interaction. If there is going to be a challenge or a problem, the supervisor also needs to be considered .

**Christian Dawson:** So, I'm going to throw out the last question from the group, before we go to closing statements, and it says, Is there any resolution to the WHOIS question? Now, let me reframe that a little bit. So, when it comes to domain registration data, it's an example of something that is quickly evolving when it comes to the use of PII. I know that NIS2 directive is something that is progressing through EU parliamentary processes, and is changing how domain registration data is shared. ICANN is going through its own processes, and the US is talking about it as well. As privacy laws rapidly evolve in the US and the EU, do we expect the framework that's put in place to be able to encompass those evolutions effectively?

**Kate Charlet:** Can I answer the last question?

**Christian Dawson:** Sure, please do.

**Kate Charlet:** I was going to just add on the trust piece of this, that another kind of pitch to the OECD government access piece, and as we're thinking about the Cloud Act and broader trust, that's a place where a lot of the conversation at a high level around government access and trust is going to get resolved, and that's the kind of thing that trickles down to some of the Cloud Act discussions. I also think it's funny that, when you're talking about challenges, that people are already prejudging the EO before it's out. I think we should spend the time to look at it and read it and interpret it.

**Christian Dawson:** I think unless somebody has a hot answer, we can go ahead and ask about final statements. Did you have an answer?

**Alissa Starzak:** I think one of the challenges when I look at what's happened on WHOIS, what we saw with the European data frameworks...

When GDPR went into effect, of course, there was a sense from US companies that WHOIS information should no longer be accessible because it was potentially subject to GDPR. Of course, what you saw with NIS2, was an attempt to recalibrate. I think the challenge as we go into that space, though, is thinking about how we maintain multi-

stakeholder models for Internet governance that are not regulatory from an individual country standpoint. WHOIS has been sort of buffeted by the winds because of the way it's been affected by regulation. Thinking about how we address those kinds of questions about making sure there is information available for legitimate access seekers is incredibly important, and we need durable solutions there that are not regulatory, necessarily, so that we continue to have a multi-stakeholder model.

**Christian Dawson:** Great point. That gets another yay from me. Let's go ahead, and Catherine, if you're willing to start us out , so today we're talking about the future of the US-EU Data Privacy Framework, what do you think is important for us to know?

**Catherine Stihler:** Well, I think it's a good day to have this discussion, I really want to thank Ruth for her remarks. I think the sooner we can have this the better, for that issue about certainty, and also to think about trust as well as we mentioned, so I'm looking forward to seeing when this comes together, which is very soon, and I look forward to the benefits it will bring both to the EU and to the US.

**David Snead:** So I don't have really any closing remarks other than to say thanks for having us here and convening, and thanks for the work that you're doing on this.

**Kate Charlet:** Likewise, thank you, and there just isn't a topic that's more important than the data flows, whether that's for the economy, for privacy, for the protections, that are necessary for those, and for all the other reasons why data flows, to support cybersecurity and resilience. Thank you.

**Alissa Starzak:** I'm going to echo everything going down the panel, and also just say thank you for being here, and being open to having a public conversation about this even before the EO comes out, we really appreciate it, and it's really useful for us to sort of understand what's potentially coming and, just as Kate said, anyone who prejudges the EO before it comes out, that doesn't work very well. So, we're looking forward to it, and thank you for hosting, and glad to be here.

**Oliver J. Süme:** Nothing more to add. Thank you so much, and thanks everyone who joined us here today.

Glad to be here, and thanks for the opportunity to speak, understanding there's a lot of details that you guys are all very interested in, that you'll hopefully soon have access to.

And I would just say, I think the range of things this conversation touched on, and the diversity of the areas and perspectives that people on this panel are coming from, really highlight that, as we think about multi stakeholder approaches, that's absolutely critical to the data and the privacy conversation as well, and governments and industry and civil society all have to be at the table to talk about these important issues, and so I'm glad to have participated in a microcosm of that today.

**Christian Dawson:** Wonderful. Thanks to our panel, thanks to our three sponsors, again I'm going to hold this up, Fieldfisher, who is our fiscal sponsor for the day, the Inclusive Tech Policy Group here at American University, and our friends at the Internet Society of Washington DC, who have brought you today's livestream, but, mostly, I want to thank my co-conveners at eco, the Association of the Internet. For those of you who are here in person, you need to grab a pair of our socks, this is the eco logo and the i2Coalition logo, and it says the leading voices in the Internet industry. eco made these for us on the event of our 10 year anniversary, we had an anniversary party here in Washington DC about two months ago, and they got us a whole mess of these socks, you should take some home.

The one big announcement that I wanted to make is that we are continuing this conversation. Two months from today, we're going to have this same panel in Brussels, and we are going to have Oliver again, and we're going to have David again, as representing i2Coalition and eco, we may have other new panelists to round out the group, and so you guys get to do this in Brussels, talk about things hopefully from the perspective of having actually seen the language. So, thanks in advance for that, and thanks for joining us, again as we cover this important topic between our organization and theirs.