THE BROOKINGS INSTITUTION

WEBINAR

TRANSATLANTIC DATA FLOWS: WHAT'S NEXT AFTER THE EU-U.S. PRIVACY SHIELD:

Washington, D.C.

Friday, July 23, 2021

PARTICIPANTS:

NICOLE TURNER-LEE
Director
Technology and Innovation
Senior Fellow
Government Studies
The Brookings Institution

SUZAN DELBENE
Member
U.S. House of Representatives

STEVEN OVERLY, Moderator
Reporter
Politico

BARBARA COSGOVE
Vice President
Chief Privacy Officer
Workday

SHARON BRADFORD FRANKLIN
Co-Director
Security and Surveillance Project
Center for Democracy & Technology

PETER SWIRE
Elizabeth and Thomas Holder Chair
Professor
Georgia Tech

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

* * * * *

ANDERSON COURT REPORTING
1800 Diagonal Road, Suite 600
Alexandria, VA 22314
Phone (703) 519-7180 Fax (703) 519-7190

P R O C E E D I N G S

MR. TURNER-LEE: Hello and welcome. We are so excited that you have decide to spend your Friday afternoon with those of us at the Brookings Institution. I am Dr. Nicole Turner-Lee. I'm the Director of the Center for Technology and Innovation the Senior Fellow in Government Studies.

And I'm particularly excited about this conversation today because there is a lot of things happening when we start about considerations of privacy legislation as well as the future of the EU-U.S. Privacy Shield. And as we have this conversation today for those of you have chimed in, I think the panelists are going to delve into the implications on trade, on innovation, privacy and security and how we need to think about particularly coming out of pandemic where we know that American businesses in particular need the benefits of cross border data sharing as well as other really unique opportunities that come with information economy that we've got to figure out how do we actually proceed with these dialogues and talks and how do we make this a win/win for everyone?

So I'm excited to host this conversation. I know some of you are thinking, you're not Cameron Kerry who primarily focuses on this. Well, guess what I've got him on the panel. And so, you will hear from many distinguished panelists who will be introduced in a moment.

But first and foremost, I have the privilege of really introducing one of my favorite members of Congress which is Congresswoman DelBene. Let me tell you why. I've had the privilege of testifying before her on the House Energy and Commerce Committee as well as the other work. I actually met her when she first came to Congress. I don't think she remembers that, but she had just really started out.

And I'm really excited because as a member of Congress she gets it and she understands the importance of this conversation today. So with formal introduction let me just say this. The Congresswoman represents Washington's First Congressional District. She current serves as the Vice Chair of the House Ways and Means Committee and she serves on the Select Revenue Measures and Trade Subcommittee. She's a strong advocate for data privacy and advocating for developing successor to the EU-U.S. Privacy Shield.

And for correction, Congresswoman I met you before the Ways and Means Committee so it's good hearing that she had infrastructure. And so, just for the record, I'll correct that.

And once we hear from the member, we're actually also going to hear from our esteemed moderator. And I'm very excited that he accepted my invitation to actually host this because for Politico magazine, Steven Overly actually covers these issues. He's very deeply entrenched in technology, policy, and politics for Politico. He reports on the ongoing development surrounding the EU-U.S. Privacy Shield on our tech companies upwards to influencing decisions in Washington. So Steve will do the honors of actually addressing and introducing our esteemed panelists.

But I just want to say to all of you, thank you for attending. Please follow this conversation on Twitter. We'll provide the hashtag in just a moment, but I also ask if you have questions to start sending them through events@brookings.edu and we will do our best within this hour to answer them. So without further ado, let me introduce Congresswoman Delbene who is actually going to kick us off with remarks and as I said she'll be followed by Steven Overly who will then usher in our esteemed panelist. Thank you very much for joining us.

MS. DELBENE: Thanks, Nicole. It's great to be here and I want to thank the Brookings Institution for hosting this very important and timely discussion on transatlantic data flows and the future of the privacy shield.

I also want to thank all the other speakers who are going to be offering their expertise on this issue and all the participants who join today because this really is an important conversation.

Data flows are critical to our shared economy future and I have seen that importance grow exponentially throughout my career as someone who spent most of my career in the technology industry. I've really witnessed the transformative power of the internet and technology. I guess, I will date myself for when I help launch Windows '95 at my first job quite a while ago. Less than one percent of the world's population used the internet.

And now, today we have more than half of the world's population online. Over four billion people and the explosion of internet users and the corresponding revolution and how we understand and

use data has fundamentally changed the global economy and transatlantic trade.

So when we're talking about the importance of data flows, we're not just talking about the traditional technology sector alone, but about how data is foundational to an increasing number of sectors across our economy such as precision agriculture or AI to boost manufacturing. In fact, 60 percent of jobs created through digital trade are in industries like agriculture and manufacturing.

And these data flows enable people and businesses to communicate online, to track complex global supply chains, to provide cross border services and support technological innovation.

COVID-19 has also highlighted just how critical data flows are during times of hardship increasing data sharing for medical research and vaccine production, facilitating video calls to family and friends, and expanding e-commerce. Data flows also have the power to provide basic financial services to billions of unbanked people who live in communities that lack the physical banking infrastructure.

And we're creating new uses of data every day. But nowhere is the digital trade relationship more important than between the United States and the European Union. Data flows are foundational to a large and increasing amount of the $6.2 trillion U.S./European economic relationship.

Unfortunately, the invalidation of the Privacy Shield framework by the European Court of Justice in July of last year sent thousands of U.S. and European businesses that dependent on data flows scrambling to find alternatives. The majority of the businesses that dependent on the Privacy Shield were small and midsized.

And as a result, many are now paying higher costs for transferred data or stop transatlantic business operations all together. The Court’s decision has not only hurt businesses, but also families, workers, and consumers in the U.S. and across Europe.

In a recent letter to the Biden/Harris administration, I urged negotiators to find a quick and lasting replacement to the Privacy Shield so that the free flow of data and trade can be restored. Although the U.S. and European negotiators are hard at work to find a workable solution as quickly as possible, I believe that Congress has to take action to help this log jam.

So what’s the single most important thing that Congress can do to ensure a lasting deal

on transatlantic data flows? We simply must enact a national uniformed consumer data privacy law. I've been very outspoken about the need for the United States to enact a federal privacy law. Personal data privacy really is a foundational issue that we must get right.

And frankly, we're already behind in creating the national privacy standard. Other countries are implementing and developing strong privacy standards. Clearly, the EEU has not been shy about its desire to have GDPR set the global standard for data protection. And if the U.S. doesn't a clear domestic policy, we won't be able to shape standards abroad and we risk letting others drive global policy.

So we need a national consumer data privacy standard that brings our lives into the 21st century. With no federal standard, states are going at this on their own. And while this is advancing the conversation in the U.S., we need federal legislation that provides a national standard of protection no matter what state you're in.

A patchwork of state laws won't work in our digital world. It would be incredibly complex for businesses especially small businesses and it won't help us in negotiating a new framework for transatlantic data flows. I authored legislation that Information Transparency and Personal Data Control Act to set a strong national standard to protect our most personal information while not putting businesses at competitive disadvantages.

The House Energy and Commerce Committee began staff level roundtables on privacy a few weeks ago. More work needs to be done to find consensus on issues such as enforcement. This is a positive step, but we have to move beyond roundtables and outlines to actual legislation and we have to pass federal privacy legislation this Congress.

So unfortunately, the invalidation of the Privacy Shield is just one example of a larger trend of data flow restrictions being enacted across the globe. The Information Technology and Innovation Foundation recently published a report that found that the number of data localization measures around the world have more than doubled in the last four years.

These are restrictions that reduce trade, productivity and make companies that rely on

data less competitive. So to combat this trend, the U.S. and Europe must come together as leaders to agree on a set of forward looking and ambitious rules to govern the digital economy and that includes the free flow of data across borders and strong consumer privacy protections.

So thank you so much for being here today for this important discussion. And I look forward to hearing from the panel. Thank you.

MR. OVERLY: Thank you very much, Congresswoman. Welcome everyone and thank you for joining today's discussion. My name is Steven Overly and I cover global trade and technology issues for Politico.

It was just over a year ago that the European Court of Justice created great uncertainty about the future of transatlantic data flows. The Court determined that the Privacy Shield agreement between the U.S. and the European Union failed to adequately protect the privacy rights of European citizens.

Since the decision known as Schrems II, it seems everyone has just been getting by. Companies have crafted standard contractual clauses to continue moving data. But questions about long-term risk and compliance remain unanswered.

American and European officials have been locked in negotiations on a successor agreement and yet complex legal and national security issues are not easily resolved.

Now, we want to hear your questions on this topic so please submit those via email at events@brookings.edu or on Twitter at the hashtag #ThePrivacyDebate.

I'm delighted to bring together four distinguished panelists to discuss what comes next for global data flows and whether the U.S. and the EU can find a sustainable solution that appeases regulators as well as judges on both sides of the Atlantic.

So to discuss that we're joined by Barbara Cosgrove who's the Vice President and Chief Privacy Officer at Workday. Sharon Bradford Franklin is the Co-Director of the Security and Surveillance Project at the Center for Democracy & Technology. Peter Swire is a professor of law and ethics at Georgia Tech and an Associate Director for policy at the Georgia Tech Institute for Information, Security

and Privacy. And finally, Cameron Kerry is the Distinguished Visiting Fellow at the Brookings Center for Technology Innovation and he was previously General Counsel and Acting Secretary at the Commerce Department during the Obama administration.

So let's get started. As we mentioned it's been a year since the Schrems II decision and companies have been operating with a lot of uncertainty around the risks of transmitting data between the U.S. and Europe.

Cam, I want to come to you first. Can you kind of tell us briefly how we got here and what the impact of the Schrems II decision has been for companies over the past year.

MR. KERRY: Yeah, sure. Thanks, Steve. So this really comes about, you know, because of the conflict between U.S. law and European law that you described.

I've done European charter fundamental rights which is their equivalent to our Bill of Rights. Recognize both privacy and data protection as a fundamental right. In European legislation has, you know, for over 25 years has brought evident the transfer of data and personal information involving Europeans outside the European Union unless the European Commission has found the legal regime in those other countries to be adequate, to be essentially equivalent to the European regime.

We don't want this between the U.S. and the EEU going back to Clinton administration and work that Peter Swire did then by arrangements that have allowed U.S. companies to subscribe to a set of principles that are consistent with EU law that are legally enforceable by the Federal Trade Commission that was the safe harbor.

That was struck down by the Court of Justice in 2015 because the commission had not -- the European Commission had not enough to look at U.S. surveillance. So then that's probably why Shield came into place. The European Commission took a close look at the U.S. surveillance laws but the conflict has persisted.

So, you know, Max Schrems the European lawyer, activist who started out fighting with Facebook about their data collection seized on the Snowden revelations to say, well, okay. You know, there's surveillance and strong surveillance by ours in the U.S. and Facebook, you know, can't keep the

NSA or the U.S. government from getting access to that data.

That was an extensively litigated second time around and ultimately what the Court said in the Schrems II decision was that U.S. surveillance authorities, the Foreign Intelligence Surveillance Act, Executive Order 12333 don't meet European requirements of the necessity and proportionality that, you know, the powers are overly broad and, you know, not on the face of the statute and protected by safeguards.

And also, you know, U.S. law on standing in federal court and the requirements of individual injury don't provide enough legal remedies against that surveillance particularly for Europeans. You know, some of those restrictions also apply in the U.S.

So that's the basis on which they struck it down. Those were the issues that we face, but, you know, the Court also went beyond the privacy issue. We mentioned there's so-called standard contractual causes. Those have been the alternative mechanisms to the Privacy Shield. There were in the case because that's something that after safe harbor struck down, Facebook was relying on transfer of data.

Many other companies do and not just American companies. Those are the main mechanisms that European companies use to transfer data around the world. And that requirement of adequacy, protection against government access now applies across the board.

So this calls into question, you know, not only transfers out of Europe to the United States, but to many countries in the world or vaguely to authoritarian countries like China and like Russia. So, you know, both you and Congresswomen talked about the importance of data flows to trade, commerce, competitiveness. You know, that is the issue that both companies are dealing with today and that negotiators on both sides of the Atlantic are dealing as they come up with a solution. And as the Congresswoman said, it's both quick and durable.

MR. OVERLY: Well, I have quite -- I'm want to come to you, Barbara, because Workday is sort of grappling with the practical implications of these sort of geopolitical and regulatory debates. You know, take us kind of inside, if you can, the company. How have you adapted to comply with the

Schrems II decision? And what has this meant realistically for Workday as you do business?

MS. COSGROVE: Sure. So this has been an issue that's top of mind for Workday and our customers. Our customers are global customers using our enterprise cloud solutions for human resources, financials, and management.

And so, they need to have confidence that they can transfer their personal data into our service for processing. We're a data processor and not a data controller. And so, we were fortunate enough that when this decision came down, we were not relying only on the Privacy Shield.

We had already offering our customers standard contractual clauses as well as binding corporate rules for data processors. And so, we were able to quickly point them to those existing mechanisms that we had in place. As both of those mechanisms remained valid post the Schrems ruling.

But at the same time, we needed to quickly get to work internally in putting together across functional groups to look at, you know, what additional supplemental measures are needed? What information will our customers need to make sure that they can uptake the standard contractual clauses and if by some chance they hadn't? Making processes easy for them to quickly add them into their agreements.

And then we've been continuously publishing frequently asked questions and conducting our own transfer impact assessment of how we thought our customers would look at the risk in terms of using our service. So looking at that case by case basis that was in the Schrems ruling.

To be able to provide them with the information that they would need in order to conduct their own transfer impact assessment. So laying out criteria like what type of data gets processed? And where are our data centers? What is the risk of a government access request?

We also took action to publish our government access principles and policies for our customers. We had had one internally but we had never had to publish it for customers. And we also published our first transparency report for customers. We had never had to publish that in the past, but for our customers to have confidence, the transfers could continue, we put one together and had it posted and available for our customers.

So it's been a lot of work and ongoing. And along the way as more information has been coming whether it's in guidance, we've been continuously updating it and trying to get it to our customers as quickly as we can.

MR. OVERLY: Just a follow up for you because, you know, earlier this year the European Data Protection Board finalized its own post-trans to guidance and updated sort of standard contractual clauses.

You know, as you mentioned you sort of used these alternative mechanisms beyond the Privacy Shield. With that guidance and with those alternatives in place, you know, I guess fundamentally do you still see a need for a successor to the Privacy Shield and you're having these alternatives take off any of the pressure in terms of reaching that agreement quickly?

MS. COSGROVE: Sure. So we were really happy to see where the standard contractual clause is in the EDPP guidance landed in the final guidance that they both adopted a risk-based approach in terms of analyzing the risk around government access. And, you know, that you can look at a company's transparency report as long as you can demonstrate a subjective. That you can look at factors related to it in the industry.

You can look at whether there's government statements around that type of data. We thought all of that was very positive and we've been, you know, pointing our customers to it and adding that to all the documentation I talked about.

And so, that's all been great, but it does not take away the need for a successor framework. As I was talking about, you know, the amount of work that we've put into -- and again, communicating with our customers and being able to rely on those mechanisms. We're very fortunate that we're a larger company. That we have the resources. That we had a robust program.

But if you think about the effort that that would take for a smaller, medium business to try and build that out and to try to answer all these questions, it's significant. And having a successor to that framework really would help a small and medium businesses.

In addition, data transfers between the EU and the U.S. are six to seven trillion dollars, I

believe. And the primary goal we need to have is to protect those going forward. Having a government-to-government agreement really will help us be set up in the long term and having more faith in terms of those transfers continuing.

And in the FCCs, the BCRs are all very helpful now. That guidance is very helpful now. But long term, we really need to see is a successor framework so that people can trust that the transfers can continue.

MR. OVERLY: And I assume that framework is being worked out now, but certainly there are sticking points for those ongoing negotiations.

One of the biggest of which I think is questions dealing with government access to data as part of surveillance efforts. I know that's been a big concern that the EU has voiced.

You know, Sharon, you coauthored an article kind of on strengthening surveillance safeguards following the Schrems II decision. Can you remind us, how far apart are the U.S. and the EU on that issue? And what does a potential path look forward as we think about creating some form of successor agreement?

MS. FRANKLIN: Thanks, Steve. And thanks also to Brookings for including me in today's conversation.

So the negotiators are not really sharing publicly the exact positioning that they're taking or the specific issues on which there are sticking points. But, you know, from conversations that we've had and understanding what's at issue, I think there are a couple of things in play.

One, of course, is the extent to which the U.S. government can enact measures to address the concerns cited by the Court of Justice of the European Union in Schrems II, by executive branch action and the extent to which we need Congress to step in to take action as well. Which, of course, as everyone knows takes longer and can be more challenging.

And as Cam outlined, the Court of Justice's opinion in Schrems II focused on two particular elements. First finding that substantive U.S. surveillance lacks adequate safeguards to meet the principles of necessity and proportionality.

And second that there's not an adequate redress mechanism for European Union citizens whose data maybe implicated. And I know we're going to talk a little bit more about redress later. So I just want to take a moment to focus on the first element which is U.S. surveillance law.

Now, of course, as an aside I should also mention that the comprehensive data privacy law that the Congresswoman was talking about would be hugely helpful and foundational to perform here. But specifically, to address what the Court of Justice's opinion focused on, we need to change our substantive U.S. surveillance to build in further safeguards.

And the opinion focused, of course, on the rights of Europeans, but really types of reforms that we would need to implement would help Americans as well. And so, I think that's important for everyone to recognize that would be across the board helpful to enact these reforms.

And there are a variety of things that the U.S. government can do through executive branch action through an executive order or a presidential policy directive that would really substantially assist in this regard. And in particular, would be reforms to collection and targeting.

So the two programs, Section 702 of Pfizer and Executive Order 12333 that were the focus of the Schrems II opinion, both involve targeting non-Americans, targeting Europeans and other people outside the U.S. But if we take steps to reign in and strengthen the standards for that targeting and collection and to really focus in on who are appropriate targets for a foreign intelligence surveillance that will help protect the privacy rights of Americans as well as European citizens.

And a couple of things that can be done reigning in bulk collection to make sure that it meets the principles of necessary and proportionate surveillance. Strengthening and narrowing the standards for targeting decisions under both Section 702 and under EO12333. And in some context really bringing in -- and to play a great role the Pfizer the court. That's the court that people may have heard of that operates in secret.

It has the ability to review classified information, but it does not under either Section 702 -- well, it doesn't under Section 702 play any role in ever viewing individual targeting decisions, but having it at least after the fact review targeting decisions by the intelligence agencies to make sure that they are

following the appropriate targeting procedures could also help in that regard.

MR. OVERLY: I want to come to you maybe to weigh in on some of those suggestions that Sharon just made and get your thoughts there. And also, kind of speak to what some of the questions or issues that this raises about U.S. national security and autonomy.

You know, I think -- or I guess I imagine that there are many in Congress and within the administration who may not be keen to change U.S. surveillance practices to appease a European Court. I wonder if you might eliminate some of those issues as well as respond to the thoughts that Sharon just shared?

MR. SWIRE: Right. Well, I think that that reluctance to have -- reluctance in Congress and the executive branch to have these things overturned on the basis of an EO court decision. It's a reason why it's hard to go to Congress to change these things.

And it's a reason the U.S. government in recent weeks has said in public that it's pursuing non-statutory approaches and seeing if they can build a system non-statutory. Or maybe you can get 90 percent of the way there without statutory and have some little perfecting amendments at the end.

And I think that's likely to be more doable. If you were going to put emphasis in Congress for action, I'd suggest the Privacy Commercial Bill that would send a really huge signal to Europe that the U.S. is coming closer to global standards on that.

In terms of the issues that we're facing, the big issue that's really, I think, negotiators have said is difficult is this individual redress idea, which to American ears might seem bizarre. So if there's Jean Claude in France. Under European law, Jean Claude should be able to go to the NSA and find out if his data has been worked on improperly.

And however, strange that might seem to American ears, their highest court has now said that in 2015 and said it with an emphasis in 2020. And so, we need to build a system if we're going to play with Europe that can meet these European requirements.

They've said the essence of a person's right that it needs an independent factfinder.

There needs to be an independent adjudicator. The adjudication has to be binding and there has to be oversight to make sure that these redress things are being followed. All that has to get built and in testimony in Senate Commerce and elsewhere I've talked about some ways to maybe build that. But that's going to take a lot of work and we hope the negotiators can make them.

But to go back to the national security frustration on the U.S. side. Here's just a couple of the points of the frustration with Europe. One is the U.S. has extensive safeguards when it comes to privacy including the Pfizer Court. And Europe hasn't really in a lot of people's views given credit to the U.S.

A second is the U.S. is way better on this stuff than China when it comes to government surveillance so why is Europe going after American companies?

A third one is that the EU is actually requiring the U.S. to be stricter than the legal rules they apply to their own governments when it comes to surveillance. And there's evidence the EU governments haven't even followed the CJEU on data retention in some of their other issues.

So there's lots of frustration from the U.S. side, but the message I would send is, get over it. Put that to one side. If we want to make an agreement, it has to be an agreement that's going to conform with what their highest board has said twice. Their rule of law approach is going to require us to figure out how to build something that meets the European rules. And if we wait for Congress to create a whole big new system, we could be waiting years and years and we'll see a lot of data cut offs, I think, before then.

So try to see what we can build now, being realistic and I think trying to rebuild the U.S. intelligence structure really is going to be a hard thing to do.

MR. OVERLY: Well, I want to come back Jean Claude and his redress rights here in a second. But first, I want to pull in an audience question on this topic that, Peter, you just alluded to and maybe Cameron or Sharon if you want to weigh in on this.

But wouldn't a replacement to the Privacy Shield be deemed adequate without the U.S. addressing these surveillance problems that were identified in Schrems II? Or will we just kind of be back

on this merry-go-round? Cameron and Sharon, would one of you like to respond to that?

MR. KERRY: Well, I'll respond briefly. Look, I think that is a risk. I do believe as Peter had said that it's possible to do things administratively. That, you know, we'd put together something that gives Europeans an independent review of, you know, Jean Claude's claims and that can provide at least some pathway to a federal court.

You know, you're not going to have full blown review, but, you know, you don't get that in Europe either. I mean a lot of the process under European law just sort of comes back and says, we've looked at the file. Everything is in order and that's the extent of access that people get.

But I do agree with what's been said that at the end of the day to ensure that the Court of Justice gets what the safeguards are, we need to make those clear in law. So if Sharon is right about some of the kinds of reforms that need to be explicit so they're not just there in the Attorney General regulations, Department of Defense regulations or agency procedures. They are there on the face of the statute for European lawyers to look at and understand very clearly.

MS. FRANKLIN: So I'd like to jump in there also. Thank you. So I think it's absolutely critical that the U.S. enact reforms and as Peter said. But I would say even more strongly the fact that other countries may have fewer safeguards in their surveillance law than the U.S. doesn't mean that the U.S. doesn't need to address the concerns of the Court of Justice of the European Union.

In my view, they're valid concerns and we need -- while there are safeguards in U.S. surveillance law, they are not adequate, and we need to make them more robust.

The other thing I do want to stress here is, I think it's important for the U.S. government to pursue a two phased approach to addressing these concerns. You know, there's much that the administration can do on its own with an executive order and it should proceed in that regard particularly with a regard to incorporating greater safeguards into substantive U.S. surveillance law.

And then we will need Congress to follow up. To codify some of those reforms and to strengthen them. And particularly that will be in regard to redress, but I know that Peter is going to weigh in the details of redress first and then I can follow up on that specifically.

MR. OVERLY: You know, I do want to pivot then to the redress debate. Obviously, that is a major issue that needs to be resolved and questions about what can the administration do on its own versus what does Congress really need to make official through the law?

Peter is someone who studied this issue quite a bit maybe more than he would even like. Walk us through kind of the biggest issues to be resolved here. And does Congress fundamentally or ultimately need to change that law or change the law in order to solve this problem?

MR. SWIRE: Well, this is one place where we don't know all of the details of discussions between the two sides.

One good thing is by executive order, the President can say to agencies, Department of Justice and NSA, whoever. Thou shalt do these things. Thou shalt comply with the decision by such-and-such a person. And that is binding. And you also can create oversight systems. For instance, the Inspectors General day in and day out do oversight in order to make sure that an agency is doing what it has promised to do. So we can have ways to create bindingness and oversight and that's clearly within the executive branch power.

The trickiest part is how do you create an adjudicator? How do you create a tribunal? Somebody who's independent enough to really look to see if it's good enough? And I don't think we've heard in public a really good account of an answer to that. But I believe people are working on that. I've been working on that in my own research, but it's a hard puzzle.

But I do think there are ways you can create adjudications within the executive branch. Maybe those get fixed better and stronger and later by Congress. But I do think there are ways forward with executive branch action.

MR. OVERLY: Sharon, what are your thoughts there? Do we need to go to Congress first? Can we start at the administration when it comes to addressing this redress question? And ultimately, if the goal is assisting an amicable agreement, you know, what really needs to happen to get that done?

MS. FRANKLIN: Sure. I think we can start with the administration. You know, Peter has

done a lot of good creative thinking and I'm very sympathetic to his goal of creating something, you know, that the executive branch can do on its own.

But I do think that to fully meet these standards of an independent tribunal that has the authority to mandate compliance with its decisions, we need to ultimately have Congress act. But, you know, Peter has pointed out some things that the executive branch can do in terms of independent factfinding. Maybe with regard to assertions of violations under Section 702 in particular where there's already jurisdiction in the Pfizer Court.

There may be some initial steps that the administration can take to move the ball forward, to show good faith to European negotiators. But there certainly is no jurisdiction, any kind of independent tribunal right now under Executive Offer 123 which is also very much implicated by the Schrems II opinion.

And even if we move toward an independent tribunal that is not what we called Article 3 Court, even if we have something, say, modeled on the U.K.s investigatory powers tribunal and create that kind of agency as the adjudicator that requires Congress to act.

So to get all the way there and have that impartial, independent adjudication that can mandate compliance with its decisions, we are going to need Congress to act.

MR. SWIRE: I think that there's a lot of logic to what Sharon is saying. One trick is that if you go to Congress and Congress writes a law to get to the Article 3 Courts, the federal courts, you have to figure out how you create standing including for maybe somebody in Europe whose never been injured, maybe never even been the subject of surveillance by the U.S.

And there was a Transunion case in the Supreme Court this term that limited standing in certain respects. The Court has taken certain an FBI case that may further limit civil review on some of these national security things.

And there are possible ways and I proposed some, you know, to try to get standing to work. But unless it's done really, really well, the standing won't work in federal court. So there's risk if you go to Congress and federal courts and there's risk if you don't. And we're going to have to find our

way through that, I think.

MS. COSGROVE: If I could just jump in quickly. I absolutely agree that the Transunion opinion makes it much more challenging to establish the standing in federal court, but you still need Congress.

Even if we don't establish this adjudication through our federal courts. Congress is going to need to create some alternative tribunal because we don't have one that exists right now that would have the inedita of independence and be able to mandate compliance to fit the (inaudible) to opinions.

So even if it is not an Article 3 Court if it's something like the investigatory powers tribunal, we still need Congress to create that.

MR. OVERLY: Let's talk about Congress. And, Barbara, I'll come to you first on this question, but others please weigh in and let's have a discussion on it.

You know, as Congresswoman mentioned earlier. Congress has talked for years about a comprehensive data privacy bill and there's been even greater pressure to do that since Europe passed its own GDPR and that went into force.

Realistically, what impact do you see a national privacy bill having on some of these big transatlantic questions? You know, it seems like creating a national standard has its own roadblocks even before we discuss issues like redress and standing and national security laws. So, Barbara, do you want to maybe weigh in on the impact of that kind of legislation would have? And then other panelists please weigh in as well.

MS. COSGROVE: Sure. It's absolutely time for us to have federal data privacy laws legislation. I've been doing this for probably over 20 years now and I feel like I've had the conversation continuously about, you know, how we have privacy built in across whether it's into HIPAA or other protections across our federal laws and built in.

But now, we're just seeing across the globe countries implement privacy legislation. And it's just becoming much more difficult to have that conversation. Even in the last two years just where we're seeing these laws come up. It just doesn't put us on an even playing field. We need federal

privacy legislation to be able to just change the entire tone and tenure of the conversations.

To be able to easily demonstrate how we have these protections in place. You know, it would be very helpful for Privacy Shield. I don't know that it's the only way that we need to get there, but it would remove a lot of the arguments around Privacy Shield if we were able to have it.

And then it also just helps us in positioning ourselves, you know, where we should be in the innovation economy. You know, aligning with these global standards will help with innovation. You know, but as we move forward, it's going to be really important for us to make sure that we are aligning with existing laws that are already in place around the globe.

Looking at principles like looking GDPR. Making sure that we're basing the laws based on the OECD Fair Information Practices. Making sure that we're looking at how we come together with other countries to develop international norms and government access to personal data as is happening in the OECD.

And having that alignment is going to be incredibly important for the durability of data transfer mechanisms even post-Privacy Shield for us to be able to see these continue on in the long term. But it is absolutely time and will be very helpful with long-term global data transfers to even looking past what we're having now with the Privacy Shield.

MR. OVERLY: Anyone else want to weigh in on the impact of the Privacy Bill?

MR. SWIRE: So here's one way. I teach privacy to my students at Georgia Tech and I have a map of the world and where privacy laws used to be in 1998, which is not very many places and where they are today.

And a couple of years ago, there were four major countries that did not have privacy laws. One was Brazil and they have their law in place now. Another is India and they're under a Supreme Court order to pass a privacy law and they're working on it. Another one is China which is surprisingly far advanced towards having a private sector privacy law.

And that would leave the United States as the main outlier globally for not having a privacy law. And it makes us look not just as an outlier, but as the single least trusting country because

we wouldn't have a privacy framework.

And that puts the U.S. now to a real disadvantage in the world's eyes when it comes to privacy. You don't want to pass laws just because everyone does it, but right now the U.S. looks really different from the rest of world and it's harder and harder for friends of the United States to make the case that the U.S. is a safe place for data to go.

MR. OVERLY: Well, Cam, I want to come to you kind of with a related question of that. But just to paint a bigger picture here for folks because Privacy Shield negotiations are not happening in isolation.

You know, we're sort of fundamentally seeing right now the U.S. and Europe trying to figure out if they can align on a range of tech and trade issues. You know, they've established this council to look at issues across kind of the board particularly emerging technologies.

To what extent can we look at Privacy Shield as kind of a test case for whether U.S. and the EU can find alignment on other topics and other issues?

MR. KERRY: Well, thanks, Steve. And I think that really kind of brings us full circle to what Congresswoman DelBene said at the outset.

And, yeah, I mean that trade and technology council that you referred to came out of the U.S.-EU Summit and the effort to -- you know, by both the Biden administration and the European Union to rebuild transatlantic relations. There can be various work frames dealing with, you know, transatlantic technology and data flows, but in broad ways. Secure supply chain, you know, climate and green tech working together on, you know, trade standards for dealing with technology and data localization.

But one of the stand out ones and it really connects with the discussion we're having today is the data governance and tech biforms. Now, Privacy Shield and those data transfers are on a separate track so that's already well advanced. The others need to get up and get rolling.

So that really is going to shape how we can work together. And, you know, to really underscore what everybody in this discussion has said, you know, having a privacy law is really table stakes in these discussions. You know, for the last year and a half I have been co-leading a dialogue that

we're doing at Brookings with a Brussel's think tank on international cooperation in artificial intelligence development and policy.

Data governance is one of the central issues there. And, you know, artificial intelligence relies on big data sets and a lot of that is personal information. So, you know, coming in that discussion really comes back to dealing with this issue of privacy legislation. And more broadly, you know, the Transitional Act Trade Technology Council and the context for that is really an effort to try to bring democratic nations together, like minded countries.

And, you know, as Peter said. The United States is now the outlier there. And in a real sense, the absence of a privacy law is sort of our original sin in those international discussions because the current system fundamentally lets companies set their own rules and puts no boundaries on data collection use and sharing.

And that results in the pressure, the lack of trust for companies like Workday and thousands of other companies that are doing work around the world. So, you know, if we're going to make this about democracy, we're going to make this about sustaining trust in global networks, you know, we do have to address these issues and respond to stakeholders around the world.

And I think that is a two-way street. And discussions like the Trade and Technology Council, I think are important to the way we do advance on so many of these fronts. I mean, you know, the European Union needs to have an open discussion with the United States and other international partners about how it's going to regulate artificial intelligence.

We need to have that discussion with the rest of the world about how we deal with privacy in the commercial arena and government surveillance.

MR. OVERLY: Speaking of the rest world, you know, I want to talk about sort of these emerging global standards around privacy. I think most notably a lot of folks have paid attention to China and its own laws that it has developed around data security and personal information privacy.

You know, I'll come to Peter and maybe then Sharon. You know, today we're talking about transatlantic data flows. You know, tomorrow we could be talking about U.S.-China data flows.

We're going to space now. Next week we'll be talking about intergalactic data flows.

You know, how complex and sort of political fraught is this conversation becoming as we see different global standards emerging?

MR. SWIRE: Well, one way to think about it is we sometimes say we're living in the data economy or the internet economy or internet age. It's not a surprise we're going to have big conflicts and big negotiations around something that important.

The big platforms are the biggest companies in the world by market share and by the number of people they touch every day. And when things get that important, China or the United States or Europe, there are countries that are going to want to have some role to play in how that's done.

The Chinese model for cyber security has been localize the data. Things can go into China, but it can't come out of out of China. There's other issues in China that people are familiar with about technology transfer and lack of intellectual property protection and all the rest.

So this is going to be a flashpoint for ongoing China/U.S. relationships. But the complexity isn't going to go away. There's a couple of hundred countries in the world. They all have their privacy laws. Brazil is going to be deciding adequacy. India is talking about cutting off data flows out of India.

This will be a central set of issues to negotiate going forward. And for global companies, they're going to have to live with the fact that in these different countries there's going to be laws. There's going to be agencies to comply with and this will be part of the price of doing business globally.

You can't just sort of put up a website and do as you wish anymore. We're much more deep into the internet age and governments are going to play a role in how the internet works in the countries.

MS. FRANKLIN: I want to agree with all my fellow panelists on the critical of importance of the U.S. enacting a comprehensive customer privacy law and how many ramifications that has for not only Americans and what the regulations will mean for us, but for U.S. relations with all sorts of trading partners or trade adversaries or competitors.

One thing to of course keep in mind is how so many of the big tech global companies are U.S.-based. And so, that again highlights the critical importance of the U.S. enacting our own regulatory scheme that controls how companies can use our data. What they can do with it. Who they can share it with? Who they can sell it to? It also has implications for, of course, our government and what access it has to the data as well.

And we're seeing in so many trade contracts -- and we were talking a little bit earlier about -- Cam was talking about, you know, the relations with the EU on AI. We're seeing reporting that various EU officials in particular have already expressed hesitance about partnering with the U.S. on regulating AI because of our lack of consumer privacy legislation and all sorts of documented cases of our government's broad use of technologies like facial recognition including from Clearview AI.

There are just so many aspects to this. And yes, in addition to the surveillance reform that I was talking about earlier passing comprehensive federal privacy legislation is also critically important.

MR. OVERLY: Well, I want to pull in some audience questions on -- and, Barbara, I'll come to you for this first one. It's related to what we have just been discussing here.

But with these current trends and different countries sort of creating their own privacy regimes. Some of which may overlap. Some of which not as much. You know, do you see the future of data flows becoming more fragmented? And is there an opportunity for convergence? And I guess if not what does that mean for companies like Workday that need to continue to move data around the globe?

MS. COSGROVE: Yeah. I'm hopefully that there will still be a common set of principles underlying the laws that we're seeing come into play around the globe that allows us to enable data transfers to continue and have base programs that can meet the fundamental privacy rights of individuals.

Now, there may need to be some nuances based on where data is. You know, differences on how consent might be collected, but I'm hoping that we still can come together and develop these, you know, international norms. The basic principles that will allow the data transfers to continue and then just know there has to be some configurability in terms of how we just develop things

around notices, consents, data access requests. But it will still allow a global program to operate.

You know, data is not segmented anymore. The interaction is here. Clouds are here. The global businesses operating and we need ways to have that data continue to flow efficiently and well understanding that there might have to be some nuances met country by country.

MR. OVERLY: Another audience question and maybe aim this one at Peter or Sharon depending on who feels most comfortable tackling it.

But the question is please comment on the EU's recent surveillance exception for child predation communications. Does this legitimize any U.S. law enforcement related to surveillance practices?

MR. SWIRE: I thought I was up to date. I'm not sure about that one. You know, Europe has had a number of situation where they've faced very concrete issues and found ways to accommodate important public interests and privacy.

And part of the difficulty is when the U.S. says, we have important interests also. It's been harder to build into the way the U.S. gets access. But let me maybe make one point that I don't think has been made.

We're sort of feeling like the poor U.S. here. And I'd like to just suggest to people. Imagine if you lived in some far away country. And most of the software you used was U.S. companies. So they're going to ship data back to the U.S. And after reading Snowden, you think the NSA has access to it once it's in the U.S.

If we were in that far away country, we might not love that about the data coming to the U.S. And that's a fear that exists in the rest of the world. If all of our data here was going to China, there would be people who wouldn't be comfortable with that access by the Chinese government.

And it's that fear and that concern which I think is understandable if you put yourself in the shoes of somebody in Indonesia or Africa or whatever it is. It's that fear that has to be addressed and I think the U.S. has to be working towards having a future where there can be statements with confidence that there's going to be fair treatment of that data.

It's the way the U.S. usually talks about it, but I think the way a lot of people outside of the U.S. often talk about these issues.

MR. OVERLY: Another question here and I'll let the panelist who maybe feel most comfortable on this one weigh in. It's really into the could industry. In particular, it says, it seems that the EU approved code of conduct regarding data transfers could be a possible solution to the Schrems case for the cloud industry. Does the panel see anyway forward here?

MS. COSGROVE: I can jump in on that one. With what's been on the trading, the European cloud code of conduct that was recently approved. Really is a means of demonstrating GDPR compliance. We were the first company to declare adherence to the code and it's officially being able to be used to demonstrate compliance.

And I think it's great. We work together with Europe and across industries to create this code. But the current code itself does not enable data transfers. It's a compliance means. There's a new module being worked on that would be focused on passport data transfers and I think it could be a great way of enabling them going forward. But it's still in its early stages right now.

I'm hopeful that in longer term as we get it finalized just like we did with the initial cloud code of conduct that it could be another means of enabling transfers. But I don't think it would take away from the importance of working on the successor framework or the federal populace station. I think all of these solutions need to come hand in hand for the code of conduct to really, really be able to enable a chance for us to continue.

MR. OVERLY: We have another audience question. Thank you all for submitting these, but here's one. If the U.S. and the EU are looking to strengthen democratic principles internationally what would be enough for the U.S. to focus its federal privacy law and consumers only or should it go broader and address fundamental rights more comprehensively? Sharon, I don't know. Maybe you have some thoughts there that you would like to share?

MS. FRANKLIN: Yeah, I mean when we think about the U.S. access to data that's an issue in Schrems. It's definitely broader than consumer. And we do need the U.S. to focus more

comprehensively.

I think one of the critical issues is the safeguards that are thus far built into U.S. surveillance law mostly are safeguards for Americans. For what we call U.S. persons. U.S. citizens and people who are legal permanent residents and then people who are physically present in the U.S.

And while we do have something called Presidential Policy Direction 28 that was issued by President Obama that provides some safeguards for non-U.S. persons, for people outside the U.S. Those are far, far, far less robust.

And so, I think that the U.S. government really needs to take this as an opportunity with the Schrems II decision. The need to restore free flow of data that is critical to so many industries and so many companies and so many consumers and so many people across the world.

To take this opportunity to really adopt meaningful measures, many of which the U.S. can do through the executive branch to improve safeguards for non-Americans and Americans alike.

MR. OVERLY: Well, we are up against the end of our panel. I appreciate the four panelists for making time to weigh in on such complex topics and I think we all recognize that even with the urgency of driving a successor to the Privacy Shield with urgency around Congress potentially enacting some sort of federal privacy standard.

There are very complex legal questions here, national security questions here that I don't think we'll find answers to as quickly as we would probably like in reality.

But I want to thank all four of you for helping to advance the conversation today and of course thank all of you for joining Brookings for today's conversation.

* * * * *

CERTIFICATE OF NOTARY PUBLIC

I, Carleton J. Anderson, III do hereby certify that the forgoing electronic file when originally transmitted was reduced to text at my direction; that said transcript is a true record of the

proceedings therein referenced; that I am neither counsel for, related to, nor employed by any of the parties to the action in which these proceedings were taken; and, furthermore, that I am neither a relative or employee of any attorney or counsel employed by the parties hereto, nor financially or otherwise interested in the outcome of this action.

Carleton J. Anderson, III

(Signature and Seal on File)

Notary Public in and for the Commonwealth of Virginia

Commission No. 351998

Expires: November 30, 2024