THE BROOKINGS INSTITUTION

SAUL/ZILKHA ROOM

TRANS-ATLANTIC DATA FLOWS: THE VIEW FROM EUROPE

Washington, D.C.

Wednesday, July 19, 2017

PARTICIPANTS:

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

JAN PHILIPP ALBRECHT
Member and Rapporteur for the General Data Protection Regulation
European Parliament

* * * * *

P R O C E E D I N G S

MR. KERRY: Well, good afternoon, and welcome to the Brookings Institution. I'm Cameron Kerry. I'm the Ann R. and Andrew H. Tisch Distinguished Visiting Fellow, the Center for Technology and Innovation here at the Brookings Institution, part of the governance studies program. And I'm very pleased to have all of you today, and to welcome Jan Albrecht for this conversation. This is part of a continuing conversation across the Atlantic about privacy, surveillance and the uses of data.

Jan has become a familiar figure to many people here in Washington as a real leader in the European Parliament on issues of privacy, surveillance, civil liberties. He was the rapporteur, in effect the committee chair, prime mover in the LIBE committee, the civil liberties committee and the European Parliament in the legislation of the general data protection regulation which will take effect next May, and has also been a leader on related issues; the review of the Privacy Shield debates about surveillance issues and others. He has been a member of the European Parliament since 2009 -- is that right?

MR. ALBRECHT: Uh-huh.

MR. KERRY: And representing Northern Germany as a member of the Green Party; an active member of that group in the European Parliament.

And so he is here as part of a delegation from the LIBE Committee to meet with people here and with our government. So let me begin, Jan, by just asking, can you tell us a little bit about those meetings; who you met with, and particularly what you are telling U.S. agencies, the White House, Congress about your concerns on privacy issues between the U.S. and Europe?

MR. ALBRECHT: Yeah, thank you, Cam, also to the Brookings Institution for inviting me and having the opportunity to talk about these issues on the occasion of our visit here with the delegation of the Civil Liberties, Justice and Home Affairs Committee in the European Parliament where until now, we had many meetings with government representatives from different departments, mainly state and justice and also, Congress representatives; also, Homeland Security, as we are responsible not only for issues like data privacy --

MR. KERRY: Mm-hmm.

MR. ALBRECHT: -- and other technology issues. But of course, also, for the whole

range of Homeland Security home affairs issues, security and police and justice, in general, which is quite a wide range of competencies, which we carry as a committee. And the European Parliament; it's more or less like many committees of Congress in one committee and in the European Parliament.

Nonetheless, of course, the issue of data protection and privacy for the European Parliament has been a very important one of the last years. I would say it's true to say that we are somehow a little bit -- those who have been pushing for these issues to be (inaudible) on the global scene, especially, of course, also in the Trans-Atlantic scene, as many data innovations, database innovations and also, businesses are based in the U.S. and coming from the U.S. to the European market.

But of course, also, because as Europeans, we have a long history of developing the fundamental right to data protection and privacy as a matter of like protecting human dignity in a like digitalized life. And that's also why the European Parliament was like pushing under my leadership for this General Data Protection Regulation to not only protect this right better, but also to have a unified standard for the European market, and therefore, also a standard which can be recognized in other parts of the world, also, in particular, in the U.S.

And that is our wish, also, as the European Union to like advertise for this kind of approach to consumer privacy protection, in particular. And by means of our like adequacy decisions, we're trying to bring in other countries and other -- businesses of other countries into respecting this as our baseline protection.

And of course, issues like surveillance practices are important there, because in order to exchange data freely, there needs to be also a common level of protection for citizens, more or less, being subject to that data. And when, for example, surveillance measures are targeting EU citizens in a far more extensive way and not limited way than for example, U.S. citizens here, when it is about foreign intelligence surveillance, for example, then this is posing a problem today. They exchange also, across the Atlantic.

And that's, of course, what we are talking about here, also, now, in order to make sure that these protections are not diminished, rounded -- extended.

MR. KERRY: So the top of the list in the press release that the LIBE Committee put out for this visit had the privacy issue. They did a transfer framework between the U.S. and the EU which is now in the process, undergoing its first annual review by the European Commission, the parliament and I think under very much your leadership had a resolution in May raising a set of issues relating to the Privacy Shield.

Last year, before the adoption of the Privacy Shield, there was a similar resolution. What are the major concerns, or what's different -- what do you see as different in the landscape today compared to the landscape before the Commission approved the Privacy Shield?

MR. ALBRECHT: I think that there are some issues which have been on our table as like concerns even after the adoption of the Privacy Shield, because of course, we wanted to have that set of rules and standards in place, so that data can flow -- personal data, which this is about, can flow across the Atlantic.

Nobody wanted to really -- yeah, shut down, transfer personal data between the European Union and the U.S. But on the other side, there is the restraint of the European Court of Justice, for example, being very strictly demanding equivalent protection of personal privacy in that country where data is flowing to from European citizens.

So we were a bit in between both of these perspectives and objectives in these negotiations. And at the end, some of the issues have been a little bit of a compromise, also, seen from the European Union's side. But at the end, of course, also, I think everybody agrees that it's good that we have reached that decision by the European Commission, and that it should also stand oppose, but that the first annual review is key to see how we can also improve this situation here and there.

What has changed, in the meantime, is basically that the uncertainty coming with the new administration is making us Europeans, of course, nervous here and there, because as I said, with some safeguards being put forward by the last administration on PPD-28, but also by Congress here and there with the safeguards on the 702 program --

MR. KERRY: Mm-hmm.

MR. ALBRECHT: -- and certain acknowledgements of the need for protection, also, of

U.S. citizens and their rights. It's a bit unclear if the level will be maintained on the U.S. side. And that is, at least at the moment, what we really are insisting on, because otherwise it will be hard for European legislators to like justify data transfers also, vis-à-vis the Court and the public and Europe to the U.S. And maybe the one or the other executive order has even made more like nervousness here and there.

MR. KERRY: Mm-hmm.

MR. ALBRECHT: Also, when it comes to some uncertainty about judicial redress rights under the Privacy Act and many issues around these data transfers in the private sector.

MR. KERRY: Yeah. Well, I understand the nervousness. I've written about some of that on Law Affair and commented on some of the ways that the negative messages that come across, but also, pointed out that you know, the fundamental elements of the commission Privacy Shield decision are presidential policy directive 28; the limits that exist by law or by executive order on Section 702 Surveillance and the purposes of that.

Did anything that you heard yesterday from anybody at the Hill or the administration or otherwise give you concern that those things may yet be rolled back?

MR. ALBRECHT: I would say a little bit of the nervousness stays, due to the fact that of course, the feedback we get from the administration is very less backed by political leadership here, as there is also a lack of political (inaudible) to lead where this is all going.

So we have that uncertainty staying in a way. But on the other side, we see that our ties between the European Parliament and the U.S. Congress and the feedback we get from there shows that certain safeguards are there to say --

MR. KERRY: Mm-hmm.

MR. ALBRECHT: -- and that there is also a firm backing of the achievements which we got. And that for example, the achievement on having the umbrella agreement being on Data Protection and Privacy and Law Enforcement Sector being adopted and implemented by the judicial redress bill is an example of how we can achieve good standards on both sides of the Atlantic to assure that there's trust in place.

MR. KERRY: Mm-hmm.

MR. ALBRECHT: And I hope that this will stay. I hope that Congress is valuing the need to also assure Europeans about the safeguards which are in place and which should be in place.

MR. KERRY: Yeah. And when we were talking in the green room beforehand, you mentioned some of the conversations that you had on the Hill about encryption, about the coming debate on reauthorization of 702.

What can you share about those conversations? What did you take away in terms of how that debate looks over here?

MR. ALBRECHT: I hope very much that on the safeguards in the 702 program there is progress being made, and perhaps, even improvements could be made for citizens not only in the U.S., but also, EU citizens, for example, when it comes to limiting purposes of surveillance and data collection or analysis.

And in particular, on the value of encryption, I have to say that from my view personally, who is also very much committed to end-to-end encryption as a solution to better protect our infrastructure and to make integrity of our systems better, Congress is even more firm on the need for encryption and the stand that there shouldn't be back draws to it than I hear it from our own government in Europe.

So I'm very much hopeful that perhaps, after years of influencing Congress and the U.S. side on privacy issues, perhaps it will work the other way around, too.

MR. KERRY: Yeah, yeah. Well, I do want to talk about you know, where European governments are headed on some of these issues. But I want to sort of stick for a minute with data transfer of mechanisms.

And as you know, aside from the Privacy Shield, there are a number of mechanisms under European law that enable data transfers to the United States and to other so-called third countries, and the most significant of those being so-called model clauses which many companies have turned to in the wake of the Court of Justice decision invalidating safe harbor.

Many of them now have you know, both Privacy Shield and contract laws in place, in case decisions again change this. And of course, contract laws as are under challenge in the Irish High

Court, and I think many people expect that case will go to the Court of Justice, as well.

And contract laws is our -- are also a mechanism for European companies to transfer data to lots of other countries; some have been determined to be adequate, some not. You know, do those countries have -- Europe right now is increasingly interested in China as a trading partner.

MR. ALBRECHT: Yeah.

MR. KERRY: What do you do about data transfers to China?

MR. ALBRECHT: Mm-hmm. Absolutely, a very important issue. I see that especially with regard to those countries where like equivalent protection is not given at all, also with regard to certain fundamental questions of rule of law and foundation rights.

MR. KERRY: Mm-hmm.

MR. ALBRECHT: In those questions and with regard to those countries, the Court will very closely look again on these issues, and maybe also make some clear requirements on the surroundings for contractual clauses. But that, of course, also applies to the Trans-Atlantic data flows, and the level will be high as in the Court's judgments before, because of course, the Court has no interest in undermining the standard which it formulates for the protection of fundamental rights --

MR. KERRY: Mm-hmm.

MR. ALBRECHT: -- for different avenues with different centers for different avenues.

So I see that this will be subject to review. But at the end, what the good thing is in the contractual clauses is that there is great involvement of the data protection authorities of the oversight bodies on this, and that there are talks ongoingly (sic) on how good protection in certain business can be achieved. And I think that's a good way to deal with it.

On the other side, I'm also convinced that we need to look further, and that of course, with the GDPR in place, you will have to comply with the GDPR, of course, in every extent when you are doing businesses in Europe. That's also important, that you see that there is a standard upcoming, and that only contractual clauses or the Privacy Shield will not be sufficient in order to do business properly, also, especially in Europe.

And when you're doing online business or business in the online environment, e-

commerce, then you can't lend out the European market, of course. So that will be important to deal with the question, how can we be compliant with these standards, and how can we be built in the future, even common standards, across the Atlantic?

And I know you know I've been coming here for years telling about the point that I would like to -- the European Union and the U.S. to build a bridge of common standards on privacy and data protection. But therefore, for a bridge, you always need like two fundaments.

And I think that although, of course, it's not very likely that under this administration things will be evolving better than perhaps, under the last one, at least my assumption at the moment, we shouldn't stop working on also introducing consumer privacy standards and rules in more generalized terms, also in the United States, in order to get closer to each other, because I'm very much convinced that there won't be a solution found only in the course, for example, of trade agreements, because we don't negotiate, for example, as European's fundamental rights in trade agreements. We set common standards.

And that will be the future for our regulatory approaches, and I hope that we will be able to get or develop ways towards it. So that's like more or less the mid-term perspective afterwards, which may be driven by the Court of Justice. We don't know, because if the Court of Justice, on the basis of our like constitutional or treaty-wise provisions, they -- that there's only one way, and that is to adjust high standards. Then we also need to do that together.

MR. KERRY: Mm-hmm. Mm-hmm.

So, let's talk a little bit about surveillance. You know, we've had -- in the wake of sort of post -- this post Snowden era as countries, journalists, parliamentarians, citizens have asked what are our own countries in Europe doing in that regard.

We've seen the adoption of sets of laws that in some sense make surveillance authorities more explicit or restrictive. In some ways, enable it to -- in others, we now have you know, the UK, France, Germany and most recently, the Netherlands have adopted new surveillance laws.

How do you see the surveillance debate in Europe? How do you -- and you know, how do you -- how do you assess those laws relative to the laws in the United States and relative to some of

the concerns that you and others in the parliament have raised about U.S. surveillance?

MR. ALBRECHT: Very uncertain, I have to say. I really think that the situation on like state surveillance -- like law enforcement or intelligence in Europe is very uncertain.

Also, due to the fact that we have a big fragmentation in the European Union where it comes to national security, that's still a field where our member states like more or less can do whatever they want, in light of European law. And that makes it very difficult to get a common understanding of what proportionate measures are -- and how to safeguard the expectations, for example, of privacy. And so that in that area and in the European Union.

And sometimes, I have to openly say that, and I did that in the past, we are having a clear double standard here when we talk about intelligence surveillance in the United States, which clearly has exceeded the boundaries of what is proportionate, which Snowden has clearly revealed.

But on the other side, we also blend out that we have similar approaches in our member states, and that of course, recent challenges by terrorist attacks, for example, in France and the UK, but also in Germany, have clearly -- or in Belgium, have clearly triggered disproportionate measures for law enforcement and intelligence thereto.

So I very much hope, as I said, that while the EU was pushing and is certainly continuing to push for data privacy and data protection in the field, for example, or consumer protection, I think that the U.S. plays an important role, and -- in making the Europeans understand that in all western societies and in all values, there needs to be clear limits, also, to stay powers when it comes to civilians.

And my impression is that for the moment, the situation is not so good in the European Union with regard to these laws. We have very different laws being brought forward. There's an emergency in France, which the enforcement acts in the UK, but we still have -- the European Court of Justice, again, which is more or less really, a solid defender of these rights.

And we have seen recently that with the judgment from December on data retention, also European Union member states have been reminded that they can't just indiscriminately collect personal data of telecommunications clients, for example, in order to then access it in case of certain events or risk, but that they have to limit, also, collection.

We have seen that on the basis of these national courts, for example, in Germany, took down the measure -- the national measure on data retention by just saying the European has said it's no go. And so we will see, perhaps, the European parliament going forward with limiting the opportunities or possibilities for member states to pass intrusive lives of surveillance, for example, in the course of the e-privacy regulation which still is under negotiation in parliament, where you also can see that the parliament wants to limit this fragmentation in the member states. So there is some light and some shadow.

MR. KERRY: Mm-hmm.

MR. ALBRECHT: And I very much hope that our continuous dialogue will also help to get the message across to our national governments in Europe.

MR. KERRY: Yeah, yeah. So you mentioned a double standard, and certainly as you know, I think that that nations rankles many Americans. What is the standard that the U.S. has to meet for sent to be -- essentially equivalent? Is it a theoretical standard or is it what the standards and practices are in Europe?

MR. ALBRECHT: I think that looking at this, we have to understand, of course, that there are very different understandings and wordings obviously in place very often. For example, when the European Court of Justice is talking about the fact you shouldn't like indiscriminately collect personal data, then if you apply that, for example, to some measures in the U.S., that's not an issue.

The collection is very broad. The issue is that there is targeted analyzed -- targeted access to this data. So there are different wordings very often, in place, and that makes it difficult to also compare that. But under the line, I think the common standards should be that there shouldn't be unproportionate (sic) collection.

There should be always a necessity test to what's happening with personal data, because we want to at the end, limit the risk of being exposed or having privacy intrusions in all areas. Otherwise, that would be without any limits and we would lose our liberties and our self determination. That's the basic thought behind it.

So that should be looked at in each and every sector, and at the end also, one important

point is that there should be individual rights and redress possibilities to it. And that is the most important issue which we have to build, especially in the field also of national security. We have had lengthy debates about the fact that if a numbers person in the State Department can deliver for that independent overview for that kind of redress for citizens from the European Union, and we will continue these talks, and we will have to continue these talks, as I said, also in the member states of the European Union.

For me, I don't make any difference there. If it's the U.S. or the EU member states, they have to uphold to the same standard, and that is at least partly being determined by the Court of Justice, but of course it's collection of different constitutional principles which we bring together here.

MR. KERRY: Good. Well, I have a couple more questions, but I do want to turn shortly to the audience and have questions -- your chance to have some exchange with a broader group of people, and your chances to have some exchange with Jan Albrecht, as well.

But let me ask you, you know, we are a little less than a year away now from the implementation of the GDPR, the Data Protection Regulation. As the rapporteur for that legislation, how do you see that process going? What do you see as the big issues ahead for implementation?

MR. ALBRECHT: I think that the biggest issue is that the GDPR is on the screen of more less everybody, which is already what some of us and me wanted to achieve (Laughter). That is at least the issue of having data protection and privacy being in every like business, in every relation of trade, for example, being respected.

And of course, that's not like the end of the story, but it needs to be interpreted by data protection authorities and courts in Europe, and it needs to be implemented, of course, by those who are actually responsible for the processing of personal data. And there we are, I would say halfway as the time to -- of these two years is halfway.

MR. KERRY: Mm-hmm.

MR. ALBRECHT: We still need much more clearance and guidance by the Article 29 Working Party, which is the collection of the data protection authorities in the European Union, to make everybody understand and also explain what the reading of this regulation is in certain sectors, as we have many new innovative data technologies.

MR. KERRY: Mm-hmm.

MR. ALBRECHT: That's very important. But also, that companies line out how they will and want to be compliant with these sets of rules. And I'm very positive about that, because I hear, for example, many U.S. companies saying that they want to be compliant and that they want to make the set of rules which laid out there to be their business standards, and that is great to hear --

MR. KERRY: Mm-hmm.

MR. ALBRECHT: -- because I think we did something from the side of the Europeans which may at the end, also be for the benefit of American consumers.

MR. KERRY: That's right. Well, I had been saying to a number of people lately that the biggest issue in U.S. privacy these days is European privacy as people deal with that. What do you see as sort of the big question mark, the big issues on which guidance from the data production authorities is needed?

MR. ALBRECHT: I think privacy by design is a very important issue, because that's a way you start with designing new products, new services. And it's the best way to be compliant at the end, because if you are going to for privacy by design, it's the way to respect these standards and values which are enshrined in this regulation.

But at the end, of course, also, the understanding how, for example, consent and opt-out work, how to define the emergence of what's personal data, of course. That's key. Also, how to work that complaints are handled by the data protection authorities themselves, so the one-stop shop which we brought across with this new one level protection in the European market will work.

So there is quite a lot to do still; also, data portability still needs perhaps, here and there, more guidance -- the new rights, which are enshrined in this regulation.

MR. KERRY: Mm-hmm. Mm-hmm. Well, let me hold sort of a couple of other questions looking ahead and turn to our audience. Yes, sir. In the gray shirt -- if you can just stand and identify yourself.

MR. BOOKER: Hello. My name is Dalton Booker. I'm a program associate at the Osgood Center for International Studies, and I was wondering, how would the Privacy Shield legislation in

Europe interact with speech that would be considered -- or content that would be considered protected, and therefore, private in the U.S. and not protected and therefore, not private in the EU? And how would the Privacy Shields handle that?

MR. KERRY: Can you give an example of the --

MR. ALBRECHT: Yeah.

MR. KERRY: -- kind of speech that you would consider protected here, but not --

(Simultaneous discussion)

MR. BOOKER: Off the top of my head, not the imagery, that that's the easy one to go to. Sorry.

MR. KERRY: Sort of a right to be forgotten question or -- in a sense?

MR. BOOKER: More a right to -- this is going to sound bad, but --

MR. ALBRECHT: No problem. I can understand it.

MR. BOOKER: -- we have the right to -- in the U.S., be for a lack of a better word, neo-Nazis, as long as we're not actively going out and harming people. And I understand that in Germany, the law of Nazi imagery is banned due to past (Laughter) --

MR. ALBRECHT: Okay.

MR. BOOKER: -- events.

MR. ALBRECHT: Actually, it's a question on freedom of speech --

MR. BOOKER: Mm-hmm.

MR. ALBRECHT: -- and its relationship to data protection issues. Oh, when it comes up that these both get into conflict. And of course --

MR. KERRY: And there's an important difference.

MR. ALBRECHT: It's very important -- different. And I think that's a very important question, how to deal with it. But I also have to say that for example, now, when I talk to Congress representatives, we see that the same questions and the same tensions are coming up with regard, for example, to -- not like Nazi speech, but like propaganda for Jihadist attacks or like hate crime and certainly sent against LGBTI or whatever you can imagine.

And these topics are there on both sides of the Atlantic. The question is how to deal with it. And there are some differences in how to handle it while in especially continental Europe. Many of these questions are solved by certain standards and laws in the U.S. It's very much in the UK, also, because of the common law system.

But judgments and precedents on the other side -- also, for example, in Germany, we'll always have courts at the end weighing the two rights. And of course, how to weigh that, and that for example, in the U.S. until now at least, the perception is freedom of speech in doubt is being given the weigh, while perhaps for example, in Germany, protection of minors from being discriminated or others is being sometimes given more of the weight.

I don't think that this is a general difference anymore, because we all have to deal with the same Internet. We all have to deal with the same understanding of values, also, more and more because of cultural globalization which took place also of our life. So my impression is sometimes that this difference is being made bigger than it is at the end.

It's more or less a difference of how to do procedure and who is competent for this decision to be taken at the end. And the general data protection regulation in the European Union, for example, lives this decision still open to the member states to handle it differently, because we don't have as the European Union, the competence, for example, to regulate free speech or free press and everything like that. That makes it a bit more complicated in Europe to understand like what's the approach. You know?

And that's a pity, I would say, but I can't change the treaties in the European Union from today to tomorrow. So we will have these like very uncertain approach, still. Nonetheless, of course, data protection authorities in the European Union are dealing with this, for example, because of the right to be forgotten when there is a request to be de-linked on a search engine because any issue being not important anymore for a non-public figure, an event which is 30 years ago, whatever -- to not be found and so on.

So they will deal with it, and I think it's important to bring in to these debates of data protection authorities also, the view of those who represent, for example, press who represent -- yeah,

the stakeholder's freedom of speech and expression and bring that together and have a talk together. I don't think it can be one side deciding on it. It's both sides which have to be recognized, and it's very small detailed decisions and weighing process in the end. And that's what I can say. I don't think that there is one size fits all to this tension between both interests.

MR. KERRY: In the front here.

MR. FORTON: Hi. Brett Forton with Inside U.S. Trade. You made reference to the ongoing debate in the EU about how to handle data flows in trade agreements. And my understanding is that the EU-Japan free trade agreement -- that there was a lot of speculation that that would be when the EU would finally kind of have a single view on this in terms of weighing the free flow of data as well as protecting the data of privacies and consumers.

I was wondering, seeing as the EU-Japan at least political deal didn't address that, what is the status of that debate, and what is parliament's role in that debate. And on a separate topic, has the commission at all responded to the parliament resolution calling for an EU review of the Privacy Shield separate from the annual review that's happening in September?

MR. ALBRECHT: So on the trade issue, I'm trying to formulate a bit that -- from the side of the European Union and especially the European parliament, data protection as a fundamental right shouldn't be like formulated by trade agreements. It's not an issue of to right -- how to define it -- the protection of a fundamental right in a trade agreement. It's an issue which you do in standards agreements like the national law and constitutions.

But of course, what is important in trade agreements is to ensure the free flow of services of products and to not have like obstacles, for example, like unjustified data localization requirements and those questions are coming up. So we see that with certain trade partners, we will certainly have to go forward and in formulating that.

But it was obviously the case that between the EU and Japan, that wasn't an issue, while on the other side, there was a chance, and that is what is endeavored now to get an adequacy decision on data protection from the side of the European Commission vis-à-vis Japan.

And that's due to the fact that Japan has passed just recently a new general privacy

legislation which makes it a very good situation for the Europeans to also say there is adequate protection in place in Japan, and that is the avenue which we choose and which has priority as seen from the European Union side, as you might understand that our approach is to get other partners in order to adopt, also, fairly high standards on the protection of personal data and personal integrity and privacy online.

This is a preferred option to just saying everybody can on his or her own side, regulate this or not, because that would at the end, not be sufficient for a full free flow of data for the Europeans. It's not possible to do that.

So for the moment, we don't need certain provisions, for example, on this issue in the Japan trade agreement because it's clear we will have the free flow of data due to the adequacy decision, and it's clear that our own data protection scheme is protected by like general guts rules, anyway.

But for the future, there may be certain situations where we also sideline with those who ask for rules on forbidding unjustified limits to data flows, like on data localization. And we will certainly work on how to formulate that in the future.

(Interruption)

MR. FORTON: Sorry. Take for instance, TiSA, where you have potentially, depending on where the U.S. falls in those 23 partners, where getting 22 separate adequacy decisions is not as practical as it is with the EU-Japan agreement. What is really, then, the course of action that the EU -- that you believe the EU should take on this?

MR. ALBRECHT: Yeah. We are certainly trying to get everybody on an adequate level of protection (Laughter), but you're absolutely right. At the end, not all of them will be fit for that. But until now, we have -- it's not our preferred option that this is the case, but we have some more time to think about that, because there is an important administration and this TiSA negotiation is not ready to continue.

But whenever continuing negotiations will come up, we'll have to also work on proposing how we want to deal with these questions, of course.

MR. KERRY: Yeah, so on the left at the back there, and then I think the gentleman over

here had a question.

MR. MURRAY: Hi. My name is Blake Murray. I cover the UK for the Department of Commerce, and I was kind of interested in hearing what your thoughts were on EU-UK post Brexit privacy world. Like do you see the UK moving towards an adequacy determination or something more like an EU-UK Privacy Shield agreement?

So yeah, I'd just like to hear maybe a comment on that. Thanks.

MR. KERRY: It's good to have the Commerce Department.

MR. ALBRECHT: (Laughter) And the big elephant from our own house, of course, which is the Brexit negotiations and what might be coming up. I have to say if something is perhaps, even more uncertain than what's coming out of this new administration, it's Brexit.

It's really completely unclear where we are heading here, and one can only talk like in the assumption of something being found as a deal, and so on. And I can only imagine how that could look like. There's three different options for the relation between the EU and the UK with regard to data protection.

One is they stay inside the single market, which of course, means to accept all of our freedoms to say that, once again. Then there's no problem with it, because the UK would implement the EU's set of rules again. Of course now, they're different than before, having no say on it, but just adopting it. Okay, fine.

The second option is that there would be an adequacy decision in place based on the EU regulation, of course. Like with the U.S. or other countries in the world, there would be a scheme worked out. And the third option is that there's nothing in place, and then you would be left with less and very few opportunities to transfer personal data, which would be clearly disruptive, as we know.

The second option is, of course, one which many people think is easy to find, but I don't think it's so, because if I see, for example, that even the DOJ, and the USA is indicating that some of the laws, like Draper or Repar in the UK are even not hitting their standards of protection of individual's privacy and integrity.

Then the UK should be really concerned about the opportunities of getting acceptance,

for example, of equivalent protection by the EU and in particular, the Court of Justice in Luxembourg. So I'm very much concerned about this field of law enforcement and intelligence in comparing them to the UK. Even if the UK would like still adopt the same rules or still implement the GDPR, it would then not be a hundred percent given that this will be happening.

So also here, either there's a clear change in approach in this area of national security and internal security in the UK, which I don't see at the moment, or one should clearly push for the UK to stick to the single market and try to do their best to be part of it and with all the four freedoms included.

MR. KERRY: So I think we had -- well, let me go to -- well, the left rear then. Yes?

MS. SPACK: Hi, thank you for your talk today. Michael Spack from CSI.

The European Commission has been discussing issuing new regulations that are trying to cut down on national data localization policies. Can you talk a little bit about the progress of that and what the prospects are? Thank you. And what that might look like. Thank you.

MR. ALBRECHT: Thank you for the question. I think you refer to a communication by the commission which is from January this year together with other issues being raised by the commission, for example, on the general policy on adequacy decisions and how to deal with -- yeah, the data economy. The question of like getting rid of data localization inside the European market is very important.

My impression is that perhaps so much legislation wouldn't be needed in that field, because with the data protection directive which is now in place, but in the future, also, the new regulation, it's clear that this set of rules is not only, and it's written in the first article, to protect personal data, but also, to allow free flow of personal data inside the European market or inside the area where these rules are pickable.

So for me, it's completely clear that like if there is no justification in the data protection rules that you can do data localization, for example, for certain national security reasons again or whatever you can find in this set of rules, then you are not allowed to do data localization inside the European Union.

And I know that there are still cases of companies who have struggled to do business in

other parts of the European market, because somehow, they are required to store data there, or whatever. But I would say that they could easily go to court and get rid of that requirement, because it's not lawful.

But nonetheless, if there is still unjustified hurdles on for example, data localization requirements, then I would certainly ask the commission to come up with legislation on that one. That is also what everybody -- the vast majority in the European parliament thinks.

MR. KERRY: Yes, sir. With the glasses.

MR. BARFIELD: Excuse me. Claude Barfield at EI. If the Congress passes the Section 702 without any change, is it a problem for Europe? I couldn't quite understand your reaction to that.

I mean, you've accepted it so far as it is. There is pressure here for change, the rights of civil liberties, et cetera. But suppose they just pass it straight out as it is, as a number of congressmen and senators want? What's your reaction, if any?

MR. ALBRECHT: I mean, to be just like very frank and open, I said it that way because I think that we did all compromise, in a way, to say that this set of rules and standards and safeguards are sufficient for us politically. While we knew, many of us knew in the European parliament and the commission, also in the council, that maybe it's not sufficient legally, because the European Court of Justice is requiring us to ask for more safeguards for European citizens.

But nonetheless, we said okay, for the moment, that's fine. But in order to be really sure that this is a solid framework which sticks also to be there and throw everybody into legal uncertainty tomorrow again, and that can be really like tomorrow, there needs to be, perhaps, some further fixing here and there in the annual review. And there was the question of having an EU review to it.

It's very important to it, because we have to see on the basis of what's happening also with some cases being referred to the European Court of Justice and some like facts about how this all is applied and practiced, if we are on a safe side there or not. But in order to be on the safe side, I think that having some more restrictions is not a bad idea. I just can say it that way.

But of course, you can't just approve it in a way as it is and hope that it will be sufficient. Politically, that might be right, but then you are still not on the safe side when it comes to the legal

requirements being set. That's the distinction which I brought up there.

MR. KERRY: Yes? Here in front.

MS. STRAPANOVITZ: Hi. Amy Strapanovitz from Access Now.

Just as a quick follow up on that question, there's also talk of them renewing Section 702 with no sunset whatsoever, making the authority permanent, which we believe removes some of Congress' very necessary oversight responsibility for that law.

But that would come probably after this review is completed in December. Will, in your opinion, the European Commission stand by its assertion that it will suspend Privacy Shield if things substantially change, if that were to happen after the review?

MR. ALBRECHT: I think that the European Commission has very little and limited margin of discretion to decided if they were going to stick to the decision or suspend it, because it's very clear that if there is any change which is diminishing the safeguards under the current decision, it will be very, very hard for the commission to uphold to it.

And then, not only legally, but also politically, because it was already a very hard compromise for the European parliament to get that accepted. Of course, the European parliament has no like formal say on what the commission does there, but the political pressure is very high.

And I can't really judge, I have to say, what significance in the assessment the sunset laws would have, but I have to say that of course, in order to do annual reviews, in order to adjust and improve the safeguards, having the sunset laws, and thereby the Congress being included into this process seems to be at least from the procedure and from the way how to approach it together, somehow important for Europeans. And I think that with regard to surveillance laws, the sunset laws are just a very good thing, and I think that the majority in Congress thinks so, too.

MR. KERRY: So yes, sir, in the middle. And one more question after that.

MR. JIN: Hi, my name is Daniel Jin. Currently, I'm a grad student at Columbia, but before, I actually worked at the Center for Information Policy Leadership with Bojana Bellamy. I don't know if you -- you probably recognize her name.

So, during my time at CIPL, one thing I noticed was there was a lot of mistrust between

industry and government; between regulators, DPAs, the commission, parliament and so forth. And industry was going one way and a lot of these regulations are going another. And there's sort of a mismatch, a misunderstanding and industry has no idea what the regulation means. Is one year even enough to comply, and so forth and so forth?

I was just wondering what your thought was on that, between this growing chasm, and given that this screen behind you says technology and innovation, you know, GDPR is -- are these laws too restrictive? Are they too strict? Are industries being forced to comply and deal with all of these legal challenges and so forth, while let's -- you know, on the other example, you have China, which has pretty much no privacy, but they're innovating like crazy.

So I just thought -- was just curious about your views on these things?

MR. KERRY: Can we have the other -- last question over here, too?

MR. LYNCH: Hi, George Lynch from Bloomberg BNA.

You touched on the Strems Two case on contractual clauses at the Court of Justice earlier. I have heard the decision is supposed to be coming up by the end of July. If you could -- if you know anything about that at the term? But if that comes out, how do you think that will impact the annual review that would come just a month after the decision?

MR. ALBRECHT: As far as I know, but I am perhaps not a hundred percent sure, the decision which is expected for the end of July is the opinion of the General Abrocot which is always the preliminary moment of a judgment of the Court of Justice in Europe.

In most of the times, the judges then follow this opinion in broad terms. Some adjustments are done. But in recent times, we also have seen that judges might also divert from that opinion. So it's an important indicator, but it's not the final judgment. So that may take some more time, also.

So it will certainly have an impact on the annual review with regard to the question also, if there is something more specific or detailed on like what's an adequate protection question and what are the certain safeguards which need to be in place, and so on. But it can't be taken like as a precondition for certain things, because that can only make a judgment itself.

I don't know how long it will take, but it's of course, important. I mean, as I said, that's the uncertain question in the room, how this legal interpretation goes on. And that is just like -- that we Europeans at a certain moment decided to write it into our constitution that there is data protection and that this is a human right, and you know, that we expect everybody to respect that, and now, we have to deal with that and we have to see where it goes.

And it will impact, of course, also, the relations with certain states and in particular, of course, with the U.S. But we're trying to get along with that, and I have the feeling that in the last years, and that goes over to the other question, we have seen significant change in how we talk about the issue of data protection and privacy, consumer privacy, but also privacy of citizens vis-à-vis the state authorities in general, but in particular, in the Trans-Atlantic relations.

I really think that has changed dramatically. I was elected to the European parliament in 2009. I came there as somebody who was like a specialized lawyer in ICT, and who has written his thesis about like data protection in the EU. And I came over here as one of the youngest members of the European parliament, talking like all their Congress members and everybody else here.

And the situation was completely different than today. It was really completely different. We had so many very different annals of perspective, including the wrong one. And since then, we have learned quite a lot; we have discussed quite a lot. So much rounds of discussions we had on this.

I think that we have come very much closer, and that includes in particular, also, industry, for example. I have had so many talks not only here, but also in Silicon Valley and other parts of the world on how industry is dealing with this question, and of course, industry never really wants regulation to be done. That's clear. You know?

And that's the same, by the way, in Europe -- also with European industry. I mean, we have other kinds of old industry, like car manufacturers and media publishers or whatever you want to see there on the field. They all don't want to be regulated. You know? But they all also have their own interests, and one of the big interests in times of like a globalized and digitized environment is also to have somehow, a level playing field, somehow legal certainty, and somehow, trust.

And we see that -- you see that in a general change of political landscape in the world,

that trust is somehow getting lost, you know, in certain issues. And that industry, businesses come to the regulators also and ask for regulation. I mean, take along Elon Musk coming up with saying AI needs to be regulated right now.

I mean, one can have very different answers on what needs to be done, but I think that there is an understanding which is common in there that something needs to be done. And then, we talk about what are we doing. And here, I think that after many talks, and we have taken five years of legislative procedure for the GDPR -- we have had hundreds of people coming in, hundreds of organizations, thousands of people coming in in this time to talk about how we should regulate or not.

And I think at the end, the feedback, which we get now after the whole debate is done and the whole process is done is that the GDPR is an important cornerstone on answering to the challenges of the digital like environment market reality in which we are, and it creates a certain set of legal certainties, and it creates a certain additional trust and guidance for everyone. And it sets a standard which at the end is set by western values rather than others.

And I think that's like geopolitically also a very important issue, as you raised China. And just to like finish by that, I was amazed about the amount of feedback I got from I got from business leadership which said that it was so important that we did that with the GDPR.

Of course, it's not perfect. There's much to be done about it, still, and there's much imperfectness in it, like in every law legislature passing. You know? But there is a very important core in it, and it is still like more or less trying to be technologically neutral and value oriented and based on the principle of accountability is still allowing for quite a lot of flexibility and innovation.

And on the other hand, through, it is really a very important cornerstone on how to get somehow a frame of regulation done. So I hope that this is seen also, as a chance to take this and use new innovative concepts, like privacy by design, as I said, like data security standards which are set there, that there's a reliable ecosystem in what we develop tomorrow.

But nonetheless, get into touch and to talks with the data protection authorities, with regulators here, FTC, FCC, about how it's going to be done together and also, with legislators, of course, if there are insufficiencies. I'm sure that with regard to new technologies, AI, Internet of Things, we will

have to talk about other approaches, also and more specific standards which might not be legislative at the end, but perhaps technical standards or codes of conduct here and there.

But I think that's a very important step, and you shouldn't see it like only as being something which is hindering us to come forward. I think it's a chance to.

MR. KERRY: Let me pick at that a little bit, just to wrap it up and on the theme of technology and innovation. Chancellor Merkel, last fall expressed concerns about achieving balance in a data protection regulation and concerned, you know, perhaps with big data. So data minimization needs to bend.

There were other concerns. You mention what Elon Musk had to say last week about the importance of getting a handle on AI. I follow your Twitter feed. You also retweeted an article on a MIT conference that talked about some of the discrimination that can result from machine learning in the AI context.

Take away from that the -- you know, is there a big -- a dystopian vision of the technological future that underlies that?

MR. ALBRECHT: Not at all. I really think that there is not, but there shouldn't also be such a dystopian view, because I think -- I'm really convinced that we are not like automatically moving into an Orwellian society and that everything is doomed because of these new technologies being developed. I don't think so.

But I think that the challenge in order to preserve our values and our society also as a free society is huge and is there by these developments, and that for example, the question, if we still are like self determined autonomists, more or less autonomous individuals in an economy doing our own decisions what we want to consume and what not, and where we want to spend our money and what not, and who we want to vote and who not, that all of that is like to be also preserved in a way, and that information technology might really endanger that, in a way.

And that still, I think that if we are putting innovation in the direction of enhancing these values in these new innovations which we develop, then I think we are on the right track, and then this thing will also create more opportunities than what we have today.

For example, anonymization depersonalization is a very important tool there, because we don't have to talk about data minimization. I think it's about the distinction between what's personal data and what's collected over me as a person, or what's all of this information which we generate everywhere.

Is it possible to minimize the effect of us as a person -- and I'm surely convinced that it is possible, and that for example, last year when I was here, I was meeting also in Silicon Valley with some guys developing self-driving cars. There is a difference if you use cameras on your self-driving car or light sensors. You can easily look at the effect of which kind of technology and which kind of innovation you are driving on our society's values and on our fundamental rights.

And I hope that we manage to do so, and I think it's very important that we are working ahead from the European, but also from the American side, together.

MR. KERRY: Good. We thank you very much for taking the time to be here. (Applause) Thank you all for coming.

* * * * *

CERTIFICATE OF NOTARY PUBLIC

I, Carleton J. Anderson, III do hereby certify that the forgoing electronic file when originally transmitted was reduced to text at my direction; that said transcript is a true record of the proceedings therein referenced; that I am neither counsel for, related to, nor employed by any of the parties to the action in which these proceedings were taken; and, furthermore, that I am neither a relative

or employee of any attorney or counsel employed by the parties hereto, nor financially or otherwise interested in the outcome of this action.

Carleton J. Anderson, III

(Signature and Seal on File)

Notary Public in and for the Commonwealth of Virginia

Commission No. 351998

Expires: November 30, 2020