THE BROOKINGS INSTITUTION

ADVANCING THE TRANSATLANTIC DIALOGUE
IN THE AFTERMATH OF SCHREMS II

Washington, D.C.

Thursday, September 10, 2020

PARTICIPANTS:

Opening Remarks:

DIDIER REYNDERS
Commissioner for Justice
European Commission

Discussion:

MODERATOR: CAMERON F. KERRY
Ann R. and Andrew H. Tisch Distinguished
Visiting Fellow, Center for Technology Innovation
The Brookings Institution

SUSAN A. AARONSON
Director, Digital Trade and Data Governance Hub
Research Professor, George Washington University

* * * * *

P R O C E E D I N G S

MR. REYNDERS: Hello, I am Cam Kerry, the Ann and Andrew Tisch distinguished visiting fellow at the Brookings Institution, and I want to welcome you to this discussion of the future of transatlantic data transfers.

We have with us today Commissioner Didier Reynders, the Justice Commission of the European Union, who oversees that portfolio. And before joining the Commission about a year ago he was for 10 years a senior minister in the Belgian government with the impressive finance foreign ministry and defense portfolios.

And we also have Susan Aaronson, who is a professor of international affairs at George Washington University and heads the digital and policy hub there and is also a fellow at the Center for International Governance Innovation which really does indispensable work in international digital policy area.

So our program today, Commissioner Reynders will make brief opening remarks. We will then have discussions and questions among the panel and we'll allow about 15 minutes for questions. I want to remind you that since we're streaming over YouTube, if you have questions please tweet with #ThePrivacyDebate or email Events@Brookings.edu or tweet to @BrookingsGov. And we have some questions in advance. Some of them I'll work into the discussion today and we'll try to intersperse those as well.

So this is certainly a timely program. In July we had the Schrems II decision striking down the privacy shield, upholding standard contractual clauses for data transfers, but imposing on those adequacy requirements for third countries and including a review of government access to information. And yesterday, of course, we saw the preliminary decision from the Irish Data Protection Commissioner saying that Facebook would not be able to transfer a store of data in the United States.

So, you know, things move forward. And, Commissioner Reynders, I look forward to your remarks and thank you for doing this — believe it's your first public appearance in the United States — and I look forward to our discussion today.

Commissioner Reynders, the screen is yours.

COMMISSIONER REYNDERS: Thank you. And thanks for your invitation and thanks to Mr. Kerry too. It's so important to discuss with you about the situation about the situation because we are currently facing on both sides of the Atlantic an unprecedented challenge for all healthcare systems, the economy, and the way of life. And the technology and data can play an important role in, for example, limiting the spread of the virus and showing business continuity and support exit strategies. The Covid-19 crisis has been a defining moment in the relationship between technology on the one hand and democracy and fundamental rights on the other. And we enter in the crisis as a democracy in Europe and the U.S. and we should exit it as a democracy, fully preserving all fundamental rights and freedoms. In addition, we need to offer trustworthy solutions to make sure that society accepts data driven tools. This is where strong privacy rules come in, and privacy is necessary to allow citizens to fully trust innovative solutions and use them without fear. It is increasingly clear that comprehensive privacy rules are key to the response to the global challenges we face today, whether in the context of the pandemic or beyond.

I see that similar debates are also taking place across the Atlantic. I'm following these development with great interest, including the virus privacy bills introduced in the U.S. at state and federal levels. For example, to specifically frame the use of personal data in the fight against Covid-19. We are seeing in the rest of the world more and more countries adopting privacy laws that reflect the same core principles and rights. It will be important that the U.S. will focus in this direction.

And I can imagine that many of you are right now focusing on the consequence of the Schrems II judgment, and I will come to that in a second. But if we take for a moment a broader perspective, it is clear that this increasing convergence in privacy laws around the world offers new opportunities to facilitate data flows.

The EU and the U.S. have been cooperating in this area for a long time based on a shared commitment to privacy and the rule of law. Privacy is one of the values that make us like minded partners. And that distinguishes us from other countries that have a very different approach to these

issues. We should work together, including with all the like-minded allies on initiatives that promote this type of convergence. Those initiatives aim at leveling the playing field for companies and defining common standards on government access to data. For example, the data free flow with trust initiative, launched by Japan is the basis also for ongoing work in the framework of the OECD. It is also against the background of this shared values that the EU and U.S. have begun exploratory talks on strengthening the data transfer framework after the Schrems II judgment.

The ruling raises complex issues, but also provides some indications on how we could address them, for instance, with respect to address mechanisms. Of course, the U.S. authorities are the best experts of their own legal system and in the best position to judge which solution to consider, or solutions maybe because we have different kind of opportunities. One of the questions is whether to build on existing elements or whether legislative changes would be needed.

I'm fully aware that these are not easy questions to resolve, especially in an area as complex and sensitive as national security. Also, it is clear that we cannot resort to a quick fix. We need sustainable solutions that provide legal certainty and that comply fully with the requirement of the court. It's a binding decision like a decision of a supreme court. The judgment raises more fundamental questions. How can a fundamental right or a constitutional right, in this case the right to privacy, be effectively protected in the borderless digital world when it takes only a few seconds to send data abroad? The debate in the U.S. around the use of certain social media and the concerns they raised in terms of access to or transfer of very sensitive data shows that this is far from being only a European problem.

According to a recent report published by KPMG about corporate data responsibility, a very large majority of Americans want their data to be better protected. U.S. citizens also seem to ask for legislation and individual rights similar to those we enjoy under the GDPR. Interestingly, according to this report, 87 percent of consumers view data privacy as a human right. I believe that compared with a few years ago, there is probably more common ground between the EU and the U.S. to find long lasting solutions based on clear rules and strong safeguards on privacy and data flows, including on delicate questions concerning the interplay between privacy and national security.

This is the spirit in which we are engaging with our U.S. counterparts. I believe you have seen the spirit reflected in the joint statement I issued in August with Commerce Secretary Wilbur Ross. In all diverse world, there is no one size fits all response to the questions we have addressed on privacy and data flows. We are working with the Commission services on a broad toolbox for international transfers adapted to different sectors, business models, countries, of destinations, and other kind of issues. It includes the modernizations of the standard contractual clauses. There are model clauses that companies insert in their contract and that are the most used transfer mechanism in Europe. We worked on this in the past months to fully align the existing clauses with the GDPR and ensure that they're adapted to the realities of today's digital economy.

The Schrems II judgment provides further clarification on the conditions under which the clauses can be used. The data protection authorities already issued a first guidance document explaining those requirements immediately after the judgment. We will continue to work with data protection authorities in the weeks and months to come as further guidance is developed.

The news we heard yesterday on the launching on an investigation by the Irish data protection and the use of standard contractual clauses, make that work even more important and urgent. We will now intensify all work with the ADPB on the development of such more detailed guidance. In parallel we will try to reflect and operationalize those clarifications in the new clauses. We believe that SCCs can continue to provide companies with an easy to implement tool to meet data protection requirements in a transfer context. This is even more important in the post Schrems II legal environment. This is important because the SCCs provide companies with an easy to implement tool to meet data protection requirements in a transfer context. We intend to launch the adoption process for the new clauses in the coming weeks and I hope finalize it by the end of this year.

I think that irrespective of whether we speak about the development of new technologies in the context of pandemic or facilitating data flows more generally, we should not see privacy as a challenge or an obstacle, rather, privacy should be part of the solution.

Another digital issue concerns access to electronic evidence. Cooperation between the

EU and U.S. in the law enforcement area could be supported by the conclusion of an EU-U.S. agreement on cross-border access to electronic evidence. This will speed up criminal investigations by enabling direct cooperation with service providers. Service providers should be clear on the rules they need to follow when requests are made from United States or European Union law enforcement authorities, thus avoiding conflicts of laws. The best way to avoid conflicts of laws, however, is to address those questions through international agreements. This is what we are seeking to achieve (inaudible) through the EU-U.S. E-Evidence Agreement and (inaudible) in the context of the cybercrime convention, the so called Budapest Convention.

The Commission is committed to work on an international agreement with the U.S. that would eliminate conflicts of law as those that arose in the Microsoft case, which then triggered the adoption of the U.S. Fraud Act. This requires ensuring that a strong set of data protection safeguards, and for (inaudible) rights, safeguards are part of such an agreement. The progress of these negotiations with the U.S. is conditional upon how the legislative process related to all EU internet rules on access to electronic evidence is advancing.

Staying on the subject of digital solutions in times of Coronavirus, I believe the U.S. to seize the opportunities offered by artificial intelligence, which is at the forefront of the response to the pandemic. But, of course, AI should also respect citizens' fundamental rights to privacy and data protection. In February the European Commission published a white paper on AI that prefers a German-centric approach. It sets out options for regulating and fostering an ecosystem of excellence and trust in the area of AI. On excellence it means investing, coordinating of research, and fostering relevant schemes, for ensuring trust. The paper includes documentation, testing, and accountability requirements. Those will make enforcing existing laws more effective and help those who deploy AI systems to comply. I'm aware that some U.S. businesses have expressed concern about use cases of AI that are sensitive as regards fundamental rights. They are calling for democracies to form a coalition of the willing to promote (inaudible) based rules on data and AI.

The U.S. also published guidelines on artificial intelligence, further cooperation of the two

sides of the Atlantic on artificial intelligence could also be possible. An EU-U.S. framework will need to promote respect for fundamental rights, including human dignity, equality, non-discrimination, and protection of privacy and personal data.

I fully support a broad regulatory convergence on both sides of the Atlantic. In June, IBM, Amazon, and Microsoft said that they will stop supplying facial recognition technologies to police forces. It is also a common goal to ensure that discrimination that happens in the offline world are not repeated and amplified by the use of AI. This is particularly important in the context of the current debate on the Russian discrimination. I also have been looking at safety and liability of AI to ensure that victims of AI technologies have the same level of compensation of victims of traditional products and services. This is important to increase associated trust in this technology and promote its uptake, as well as to maintain trust in the justice system.

Lastly, a few words on consumer rights. During the Coronavirus pandemic we saw a sharp rise in remote traders promoting false claims or scams products. Many consumers were misled to buy overpriced, ineffective, or potentially dangerous products. In response we coordinate with the network of EU member states authorities a screening of online platforms and ads. And we shared guidance on the most common illegal practices taking advantage of the COVID crisis. I reached out to major platforms, including Amazon, AlliExpress, Microsoft, Bing, eBay, Facebook, and Google, asking them to cooperate and address the identified misleading content. The platforms responded positively and have removed millions of misleading and illegal ads.

But the fight against online (inaudible) traders will not be over with the pandemic. All the threats consumer vulnerabilities will be used, as well as methods to defeat automatic checks. And this at the world level. Transatlantic cooperation should therefore be strengthened to share knowledge, best practices, and innovative investigation tools. I will work to strengthen the cooperation between the EU network of consumer protection authorities and the U.S. agency in charge, the Federal Trade Commission.

In conclusion, the Coronavirus crisis has hit both the EU and U.S. hard. We must remain

strong international partners and work together. It means stepping up efforts to provide true and transparent information about the virus and related health products to ensure that consumers feel safe. I also committed to working together to promote and further develop convergent solutions for the use of artificial intelligence. I will also continue to discuss with our U.S. partners to find solutions for a strong data transfer framework that ensures the smooth flow of data for all Transatlantic digital trade. This is essential for the EU and the U.S. to reap the benefits of the global data economy. And I look forward, of course, to talking more about EU-U.S. digital policy in our panel discussion.

So thank you, Sir Kerry, for such an invitation. I know that you are focusing now maybe on the Schrems II judgment, but I'm sure that we have a lot of other things to do in common between the U.S. and the European Union, and we are working on it.

It's maybe my first public appearance, like you said, in the U.S., but I was already as new commissioner in the U.S. in December last year to meet the attorney general and the Department of Homeland Affairs to start the discussions of all those issues. Now, of course, we are continuing to do that by video conference, but with the same commitment, I assure you.

MR. KERRY: Yeah. Well, Commissioner, thank you very much. And, yes, there is a range of issues to discuss and certainly a lot of meat to digest in your comments on those. And I think anticipates some of the question that Susan and I have, as well as members of our audience.

I certainly appreciated your discussion about collaboration on AI. It's something that we have been working at Brooking with the CEPS think tank in Brussels and leading a dialogue with the Commission, UK, Canada, and U.S., as well as numerous stakeholders and experts on how we can collaborate in AI development.

And I was also encouraged by what you had to say about convergence, but, you know, not approaching things with a one size fits all approach. I mean I certainly view some of the challenges between the U.S. and the EU on data issues a really stemming from cognitive dissonance that comes from common law thinking versus civil law thinking and how we think about law.

Susan, I know you've focused a lot on sort of trade issues and convergence and have

some questions about how we deal with that. So let me turn it over to you to explore that with Commissioner Reynders a little bit.

MS. AARONSON: Thank you and thank you so much for organizing this and thank you, Commissioner Reynders, for speaking to us.

Briefly, could you talk about EU perceptions of interoperability and adequacy — two very different terms — and how they might change given the Schrems II decision?

COMMISSIONER REYNDERS: About the Schrems II, maybe just to say that first of all I said it's a binding decision, so we will try apply. And I was very pleased to see the reaction of all U.S. partners to say the same. And so we want to be sure that it's possible to apply the decision.

Sometimes on the basis of the actual legislation on both sides, sometimes maybe we some change in the U.S., but I said it's first of all the U.S. authorities that they had a good place to see what are the needs to change or not. But certainly about the national security issue, I know that this is a difficult element. But I want to confirm that without the privacy shield — because now we are working without the privacy shield — it's important to continue to work with the standard contractual clauses and we are working on that with the board at the European level, the network of national data protection authorities.

And I've said in my remarks I know that you have also seen the situation in Ireland yesterday, but it's an investigation, it's not a decision, you know. I've seen the declaration from the people of Facebook and (inaudible), but until now they are investigations in Ireland and not yet a decision. And we are working with the EDPB about the (inaudible) in Europe to see what kind of other tools are possible to use, because of course you know better than I the situation now with the election in the U.S. So I'm sure that it will be difficult to have some legislative change in the next weeks, but it's possible to continue to work on the modernization of the SCCs and then to see if we have the capacity to reach an agreement on some change.

And so you spoke about interoperability. I want to say that the concept that we have in Europe is that of course we have put into place a protection for the personal data with the GDPR and we

tried to be sure that the protection is traveling with the data. When we are open to send data to a partner, we want to be sure that the protection is traveling with. And so it's not first a trade issue. The GDPR and the data protection is first a protection for fundamental rights for the citizens. And, of course, it's not just with the U.S., it will be with the same approach with all the partners. We have a lot of adequacy decisions with different partners, like Japan, to give an example, and we are in discussions with South Korea, but we also discuss with UK, because you know due to the Brexit.

So, again, we are very open to promote the GDPR. On one side we have protection for the personal data, on the other side it's very open to exchange data with other partners. But, again, we want to be sure that the protection is traveling with the data and that we have the same kind of protection. And it's the reason why we take the adequacy decision or not. And, you know, the privacy shield, it wasn't adequacy decision, but at the end now we have a decision of the court and we need to apply and to find a way or to go to a new adequacy decision after some change or to apply other kinds of mechanisms.

MR. KERRY: Thank you. I'm — did you have a follow up, Susan?

MS. AARONSON: How do you relate that to the notion of interoperability, given that it is a fundamental right, but it's also normative among countries? Will the EU's approach to interoperability change at all in relation to this? I guess the bottom line of what I'm trying to say is that I don't see that much focus on interoperability of regimes, it's more, you know, that because it is a fundamental right it must be protected at all costs, and hence the EU approach is dominant.

COMMISSIONER REYNDERS: But it's true that the protection is dominant, but I've seen also an evolution in many parts of the world. If you look to the evolution in Brazil for the moment. I spoke about South Korea. But also in the U.S., I said also in my remarks I've seen some new initiatives in California, maybe — not in Washington, D.C., but in the Washington state about some possible new protection for the citizens. And I'm sure that we will have more and more common approach. And it's maybe just for the discussion on this international level, I mentioned the initiative of Japan to start something on that. But, of course, the most difficult issue is maybe in relation with the national security.

And you have seen in the elements of the decision from the Court of Justice about the Schrems II, it's that there that we have some things to do because we don't have exactly the same approach about the capacity to collect some personal data for security reasons or intelligence reasons at the national level. But there are also some possibilities to see if we have the same kind of protection, comparable protection and, certainly, is it possible for the citizens to enforce their rights. That's the sort of question that we have with many partners. We don't want to be sure that it's exactly with the same rights, but we want to be sure that it's comparable and that it's possible for European citizens to enforce their rights before a court in the U.S. or UK or Japan or in other countries, like for the national citizens, like for, in your case, the U.S. citizens.

And on all those issue there are some possibilities to have room for (inaudible) because I'm sure that there is some more and more — there's an increasing request also from U.S. citizens to have a better protection. And I have seen sometimes in the political debates, I said that I saw some discussions with the platforms and with the right to use the personal use. And I insist it's about the personal data. We have many other data and we'll have more and more other data in the future, with all the same protection because if there's business to business, these other kind of actions. And so we need to think about the way to have an evolution on all those issues.

But, again, we tried to be sure that the protection that we are giving to European citizens is traveling with the data when we transfer data as well.

MR. KERRY: So, Commissioner, you mentioned the increase in comprehensive privacy legislation and certainly a drum that I beat here in the U.S., but the real focus of the ACJU's decision deals with intelligence, surveillance, and the scope of U.S. authorities in traditional authorization and the remedies available to EU citizens. I want to explore that a little bit in terms of what it will take, although I think you have deflected the question that I had (inaudible) at Politico, and you had, as to whether this will take — need U.S. legislation on intelligence.

But I also want to explore a little bit some of the broader implications, because certainly the decision imports adequacy requirements into SCCs and puts on companies, both exporters and

importers of data, the burden to assess the laws of third countries with respect to (inaudible) access. How are they possibly supposed to do that? I mean look at the process. The Commission has been through the challenges of doing that and yet you do have little countries out there that — you know, China certainly a leading example that have very broad surveillance — so how do people deal with that, how do you anticipate — you may be able to deal with that in SCCs.

And more broadly, to pick up on a question from Marc Rotenberg, a long time privacy expert, you know, how does China affect the broader issues of U.S.-EU collaboration in the digital —

COMMISSIONER REYNDERS: But, first of all, to be clear, we don't have and didn't have an adequacy decision on China. You know that we don't have to decide. So, yes, it's a huge difference. No, we are discussing about the way to have a specific relation with some partners through adequacy decisions. We will work maybe with modernization of the SCCs. But, again, the SCC — of course it's possible to use, but with certain guarantees about the functioning of the internal protection for the personal data in the partner countries. So we don't have the same kind of use with China that it's possible to do with the U.S. And if we are entering now in a discussion with the U.S. about what is the next step, is it possible not only to confirm the use of SCCs in the near future with the modernization, but to go to some adaption in different legislations. That's the way forward. And we don't have this same discussion with China.

And when I'm looking for maybe a broader approach, I must say that except the discussion at the EU level, we have some discussion in the concern of Europe. You know that. We have also some elements of possible evolution at the level of broader Europe. But we are also in discussion with — I said the proposal of Japan, but the proposal of Japan will be maybe first with the U.S., with Europe, with Canada, with, of course, Japan, but not China s a first possibility because, of course, we have more concern about the way to organize the national security and the functioning of the (inaudible) services maybe in other countries and in the U.S.

And there's a reason why I insist on the good collaboration, because if it's possible to find a way to have a common approach between the U.S. and Europe on different fields. It's the reason why I

spoke also about artificial intelligence, attribute the real basis to try to to have international standards. If we don't have the capacity to conclude some agreements between the U.S. and Europe, of course we let more space to others. And it's true that we will let maybe more space for influence coming from China or other partners. So the relations among the U.S. and EU is very important. It's the reason why I said it was my first visit before the crisis, before the pandemic, it was to Washington in December to start a discussion on all those issues. And we have said we need to continue to enhance our capacity to work closely.

But, again, we are in such a discussion because we had an adequacy decision on the U.S. and we tried to have another one. We don't have with China, of course.

MR. KERRY: Right. Susan? And then I think we'll try to move to the audience Q&A and we'll go maybe —

MS. AARONSON: Can you talk a little bit about digital sovereignty as a concept? And would you view American's ban — both the House and Senate have now banned TikTok — of TikTok and WeChat as examples of digital sovereignty?

Thank you.

COMMISSIONER REYNDERS: Well, there are many discussions on sovereignty in general and, of course, more so now with digital sovereignty and the need to see if it's need to localize the data on your territory or not.

I will say that I'm sure that the concept that we have put in advance in our communication in February about artificial intelligence is that we want to invest in the digital world and we want to have a better data strategy at the EU level. But the principle is to be sure that it's possible to apply the same rules everywhere. And so we don't want to have a localization of all the data on the open territory. Of course want to promote the capacity of Europe to develop some activities and to develop strategy and storage of data and management of data, but if you are coming from abroad and you are coming with your own data, it's also possible we're just asked to apply the same rules or comparable rules than the European. And it's there reason why we have the same approach when we transfer data and we want to

have the same protection. If we receive some actors using their own data we want to be sure that there is no discrimination in the way to organize the use of AI on data, there are no violations of fundamental rights and so on.

So it's not to say we want to have a protection and we want to build a real sovereignty at the level of the European Union and that. Of course we want to be stronger than before because we are knowing that we have a lot of things to do to invest in the digital world, but we are open and we still stay open to others, but, again, with the same approach. We ask to all the different partners to come with the same kind of approach about the human-centric approach. I mean no discrimination in the use of the data by new elements like expert system or learning machine and so on, and no violation of fundamental rights.

And if I may, because I know that you are putting the emphasis on trade and the link between trade and data flows, again the GDPR, it's for protection (inaudible). But I want to insist on one point, I have seen a huge difference between the companies at work in the digital world — and to be concrete, Schrems II is about Facebook — and we have seen that there are companies at work as a platform with the use of personal data. But there are many other classical industrial companies and they don't have exactly the same concern because they don't need the same level of transfer of personal data and insist on the fact of personal data to another part of the world, when if you try to organize your business in the car industry or the food industry on another continent, you don't need the same transfer of personal data. Then if you are organized, a real platform, trying to work with personal data of all the users of the platform. And that we will also discuss with the industry. And I'm sure that it's important also to discuss with industry in the U.S. to see what are the requirements of the different categories of companies. Because it's maybe easier to use standard contractual clauses for some actors with all the same requests to transfer massive personal data, then for those active in the management, in fact, of personal data due to the fact that their platforms with users like dedicated to that. And I've seen that because I've had a lot of contacts with CEOs of companies. And we don't see the same concern, to be concrete about Schrems II, if you have a contact with — say you are at work exclusively in the digital

world with a platform or if you discuss with classical industry. And that's a sore difference, because when you spoke about trade, you need to make such a difference and so. And I'm sure that there is some room or manner for other kind of tools to exchange data flows and to exchange data among companies in such a way.

MR. KERRY: Okay.

COMMISSIONER REYNDERS: I just thought it's so surprising —

MR. KERRY: So we should move —

COMMISSIONER REYNDERS: It's so surprising that the Schrems II decisions about Facebook.

MR. KERRY: Yeah. So we should move to some audience questions, but before I do that I want to put a question to both of you. We seem to be — but, you know, to pick up at the end of the program a little after 11:00 — we seem to be moving at five year intervals. It's been five years since the first Schrems decision, you have a five year mandate, Commissioner, and it seems like every justice commissioner has to negotiate some deal with the United States. So five years down the road, what will this discussion look like? What would a Brookings program on EU-U.S. data transfers look like?

So let me with that put a question that — and put you on the spot a little bit, Commissioner, because I think there are some more concrete questions about the discussions. You know, from Mike Swift at Mlex, how you see this negotiation as more difficult than privacy shield and, you know, which was more difficult than safe harbor.

And, similarly, are there changes to FISA Section 702 or to Executive Order 12333 that are part of the discussions as to how the U.S. responds more to the court's proportionality concerns. So that's something that comes to us from Greg Nojeim at CDT, Center for Democracy and Technology.

So now you're on the spot, Commissioner.

COMMISSIONER REYNDERS: Yes, but first of all, I want to say that we have a good collaboration with our U.S. partners since not only the Schrems II decision, but maybe before because we have had discussions in the first months of this year about the possible decision and the way forward.

And, of course, we are knowing that it's very important to give a certain level of certainty to the company. So that is the reason why I said we are in close contacts with the European Data Protection Board about the modernization — I don't want to repeat it — of the SCCs. That's a possible element.

Then, of course, if we want to give a concrete answer to the court, it's also important to analyze the possible legislative changes in the U.S. about different elements. I spoke about national security, intelligence, so on, but you know that we have had many discussions about the ombuds person. What is the scope of the possible actions? What is the capacity to intervene? And that's a real issue. Not to have exactly the same mechanism in Europe, it's not the request, but have the same level of protection. Is it possible to discuss on the way forward. And said to the American authorities are in the best position to analyze that and to see what other possible moves.

But, on the other hand, it's also very important to see what kind of enforcement is possible for European citizens about their personal data sent to the U.S. And is it possible to have the same kind of level of enforcement as the U.S. citizen. If you have some possibility to go to justice — again, I'm Commissioner for Justice — it will be an important part of the process.

And so it's possible to build on actual existing elements in the U.S. I spoke about ombuds person and different kinds of actual possible mechanisms in the U.S., but maybe also about some possible change. And, of course, it will be more and more important if you have the same request for the protection of personal data coming from the U.S. citizens, because I said I've seen the new evolution in California and other states. If there are some evolutions at the federal level, of course you will give some rights to the U.S. citizens. Is it possible if you are doing that to give the same kind of protection and the same kind of possible enforcement to European citizens having their data transferring to the U.S., like for the U.S. citizens in Europe of course. If we organize a transfer of data from the U.S. to Europe, is it possible to give to the American citizens the capacity to enforce their rights?

And so I'm sure that we are working on different levels. Of course, at the technical level certainly the SCCs that is the mechanism, but we work at the level of the common vision of the protection

for that personal data. And, again, there are I'm sure some evolutions on some size in this way. And then what kind of enforcement of that. And, of course, national security, I know it's a very sensitive issue and that is more complicated. I'm fully — I'm sure that there we need to be very prudent. But I've said also that we tried to work on the E-Evidence and on an agreement between the EU and the U.S. because there's a difference between the exchange of data among companies, also in the way to work about the evidence, and the law enforcement authorities of course. We have different rules for the law enforcement authorities, and there are some possibilities to do more. But we try to find a way to a solution at the EU level first, but the access to E-Evidence for the law enforcement authority in Europe, and then to see if it's possible to conclude some agreements with the U.S. on that.

But, again, the most important elements to see the evolution in the protection of personal data in the U.S. and then the capacity to enforce the rights given to the European citizens, like you will have maybe an evolution about the rights of U.S. citizens in the same field.

MR. KELLY: So we have several questions about adequacy decisions, and particularly Fernanda Nicola of American University asks about effectively what will be the transparency of the Commission review of existing adequacy decisions that you have on your plate, the review in light of both Schrems decisions for some countries with intelligence programs, Five Eyes partners, Israel, and others. And of course you've mentioned as well the pending adequacy decisions, so what will be the level of transparency on those and will there be Commission decisions in the reviews that could be reviewable by the CJU or that would inform the application of SCCs?

COMMISSIONER REYNDERS: First of all —

MR. KERRY: And, similarly, just to reflect a question line from Elaine Fahey, how do you anticipate changing those reviews given what has been the clear sort of differences between the Commission's adequacy decisions and reviews and the views of the CJU?

COMMISSIONER REYNDERS: First of all, we have organized an evaluation of the GDPR after two years. It was the second anniversary of the GDPR. And before the summer we have explained the evaluation. But I have said also that it was possible to postpone the evaluation on the

adequacy decisions due to the fact that we were waiting for the Schrems II decision. Now we have. And so we will fully apply the requirements of the court in the review of the existing adequacy decisions, such as with Canada or Switzerland, to take some examples, and that we are currently evaluating. So we will see if we have some concerns about the way to apply also the conclusion of the court, the decision of the court, on the — and the requirements of the court on the existing adequacy decisions.

We will also apply those requirements for the new adequacy decisions. I said that we are for the moment discussing with South Korea and, of course, we'll see if it's possible to put the same kind of requirements in the discussions about the adequacy decision. And the same due to the Brexit with UK. And we are working now to collect more information about the way forward in UK, about the protection of personal data.

And to the extent that issues would emerge from the evaluation of existing adequacy decisions, the relevant report will identify measures to resolve that. So we tried, liked we discussed with the U.S., to ask maybe additional safeguards agreed with the concerned country. So if we have some concern, to be concrete, about actual adequacy decisions in Canada or Switzerland, we'll ask to have an agreement on new safeguards. If we have concern about a possible situation in UK, we'll do the same.

And, of course, I must say that it's possible to go to a suspension or a termination of certain adequacy. And you spoke about the transparency, of course we will have a transparent process and it will be possible for the citizens of the organization to go to the court. And the ECG has the same capacity to act of course about all the adequacy decisions, like it was possible to act about the adequacy decisions with the U.S.

And so suspension or termination of certain adequacy decisions is a possible outcome if our assessment would reveal certain problems in the level of protection that cannot be resolved. So we have the same kind of situation and we need of course to ensure continuity. But the first element is to see if it's possible to have additional safeguard if it's needed. And I'm sure that in the next discussion with some partners it will be possible to do that and to avoid of course a suspension or a termination. But we are not sure. And you have maybe followed the discussions with UK for the moment. We have

difficulties on all the field than just about the transfer of data. So I don't know what should be or could be the decision at the end of the year. I prefer to have a smooth process and to have a good agreement for the future relations between EU and UK. I'm sure that the data transfer is an important part of a smooth process and a good agreement, but I don't know. That depends on both sides of course.

But, again, it will be transparent, we will come with an evaluation, and it will say if we need new elements on the basis and the requirements of the court. We will apply exactly the same reasoning with all the partners that we are ready to do with the U.S. for the moment.

MR. KERRY: So we have a couple of technical questions, which I want to put in the context of review of SCCs and sort of what sorts of measures may work to enable data transfers. One from Zabia Verso (phonetic) at the French embassy on federated learning tools, so tools that allow the sharing of access to data for inquiries but without sharing the data. And then from Gary LaFever at the company Anonos, which works on anonymous transfer solutions, German DPA guidance on the use of anonymization or encryption or pseudonymization where a data exporter retains the keys. Are those things are being examined as part of the review of SCCs and potential mechanisms for additional safeguards under the court's decision?

COMMISSIONER REYNDERS: Yes, but first of all, due to the fact that we are working as I said with the European Data Protection Board, so the Board were sitting all the different national data protection authorities. So if there are some proposals coming, like you said, from Germany or from other data protection authorities, it's a part of the discussion.

But the main issue about the SCC is, first, work done since many months about the modernization due to the fact that we have worked with SCCs before the GDPR. And we need of course to take into account the GDPR in the modernization. That's the first element.

The second element is, of course, the new technologies that we have now. And, of course, we need also to take into account the evolution of the technology. And the third one, the requirement coming from the decision of the court. And it's on such the last part that there are some ideas about effective mechanism to fulfill all the requirements of the ECG. And it's the reason why I've

asked from the beginning not only to work with our U.S. partners, but we are working with Mrs. Jelinek — you said you have seen (inaudible) about this from Mrs. Jelinek — I'm working with Mrs. Jelinek and the Board from the beginning to be sure that there's a common approach from all the national data protection authorities on the way forward. And it's the reason why, of course when we will come at the end of the year with the new SCCs, we will have formal advice from the Board.

And so, again, all those technical proposals are in the examination of the possible modernization because they are coming from the national data protection authorities and we are working with a network of the national protection authorities. Of course, it will be possible to follow some proposals and not others. We will see. We'll try to have a common approach of all the national protection authorities.

When we have complex issues — and the Schrems II, it's a complex issue, of course — we want to organize a process to have a common approach in the entire Europe, so with all the different actors. There's a reason why I insist. I've listened to your interdiction and to say that you've seen the decision of the Irish authority yesterday. It's just an investigation, you know, and I've seen the declaration coming from Facebook, but the official position of the DPA, it's an investigation and we are working on it.

MR. KERRY: Yes. Well, we need to come to the end. So five year predictions — I'll go first to kick it off for a few seconds. You know, I believe we have to prepare for the worst but hope for the best. So we need to keep hoping we will have comprehensive federal privacy protection in the United States, we will have surveillance laws that incorporate the protections that exist for international citizens and numerous other safeguards, we will have a robust data flows framework, and that Brookings program will be talking about the successes in international collaboration on things like climate science and epidemiology and the like.

Susan, your prediction?

MS. AARONSON: I predict that there are going to need to be rules governing the mixing of public, personal, private data in plans. I think that AI strategies and data plans are going to be better integrated.

I agree with you that we're going to have a national privacy law in the United States, but, Commissioner Reynders, you made an important point, and I would love if you could expand on it, which was about differences between metadata for companies, such as let's say Ford Motor Company, using (technical inaudible) versus a Facebook (technical inaudible).

MR. KERRY: Commissioner Reynders, I don't have time for that, but you have the last word.

COMMISSIONER REYNDERS: No, but some elements may be as if we are going to the next years. First of all, I'm hoping that it will be possible to organize a new webinar in five year's time, not only because we will have a physical presence and not a video conference, but certainly because I don't want to speak about a Schrems III decision (laughter) after five years. So that's a first element as for your projection. Please not with a Schrems III, so we need to find solutions.

The second element the same. I'm sure that we will have an evolution in the U.S. about the privacy and the protection of personal data. And if it's the case, the state level and the federal level, it will be maybe possible to have a common approach to convince other partners to go in the same direction and to have more and more international vision and to have more and more international standards about the data protection for the personal data.

And, of course, the most difficult issue I'm sure is to see what kind of evolution in the field of national security and the different possibilities for the intelligence services and the law enforcement authorities to have an access to personal data. And there I said we need to work about the way to enforce the individual rights about the data protection. And we need to think maybe with the U.S. about the way to reinforce in the next five years the capacities of the ombuds person in the U.S., if you have an evolution of the same rights for the U.S. citizens in the protection of their personal data. And then always possible to give the same capacity to enforce their rights to the European citizens, then to the U.S. citizens in the U.S., like we tried to give the same enforcement of their rights to the U.S. citizens in Europe than for the EU citizens. Those are the main issues, because we don't want to have exactly the same mechanism or the same rules. We want to have a possible cooperation and to be sure that we have the

same kind of protection. But if you give a new protection to U.S. citizens, it will be easier, of course, to give the same protection to EU citizens and it will be more a problem of enforcement of the right than something else.

And, again, it's possible to have another vision about the national security issue on both sides of the Atlantic, but we need to be sure that we are giving the protection to the people and to give the same capacity to enforce such a protection.

And, of course, if we are doing that, again, it will be possible to avoid a Schrems III decision and to work with adequacy decision and to work with a very sold basis for all the companies. I've just expressed the fact that I've seen the difference between the companies that work quite exclusively in the digital world and all the companies in more classical industries. But we tried to find solutions for both. And I'm sure that in five year's time it must be possible, not to just work with SCCs, but maybe to go to a new adequacy decision due to a positive evolution in the U.S. about the protection of personal data and a better understanding about the way to enforce the rights of the citizens on both sides of the Atlantic.

MR. KERRY: Well, Commissioner Didier Reynders, thank you very much. You certainly have your work cut out for you to deal with all of those issues with the urgency you described.

Professor Susan Aaronson, thank you for joining us today and thank you all of our audience for being here today.

COMMISSIONER REYNDERS: Thank you. Bye bye.

* * * * *

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