THE BROOKINGS INSTITUTION

HUMAN RIGHTS AND DATA:
VIEWS FROM A LEADER IN THE EU PARLIAMENT

Washington, D.C.

Thursday, July 19, 2018

PARTICIPANTS:

CAMERON KERRY, Moderator
Ann R. And Andrew H. Tisch Distinguished Visiting Fellow, Governance Studies
The Brookings Institution

SOPHIE IN 'T VELD
Member
European Parliament

* * * * *

P R O C E E D I N G S

MR. KERRY: Well, good morning and thank you for coming. I'm Cam Kerry. I'm the Ann R. and Andrew H. distinguished visiting fellow here at the Brookings Institution. I want to welcome you to our conversation with Sophie in 't Veld of the European Parliament. I remind you to please silence cell phones, but feel free to use them to live Tweet this event with the hashtag up on the screen.

Sophie in 't Veld has been since 2004 a member of the European Parliament from the Netherlands, a member of the ALDE Group, the group of Liberals and Democrats in the European Parliament. And in particular, for most of that time she's been a member of the LIBE Committee, the justice and civil liberties committee of the European Parliament, so the equivalent of, I guess, our Judiciary Committee. Is that who you regard as your counterpart mostly?

MS. IN 'T VELD: It's Civil Liberties, Justice, and Home Affairs, so it's very important.

MR. KERRY: Yeah, right. And in that capacity, has been outspoken about civil liberties issues, particularly about surveillance. She was certainly in the forefront of critics of U.S. surveillance, both before and after the Snowden revelations, but not just on surveillance issues. Issues of LGBT rights and immigrant rights and others. So I expect that we're going to have a pretty outspoken conversation.

So, Sophie in 't Veld, welcome.

MS. IN 'T VELD: Thank you.

MR. KERRY: You come at a pretty extraordinary time in transatlantic relations after all of the events last week in Brussels, in the U.K., and in Helsinki. So talk a little bit about that. And, you know, you're here with the LIBE Committee and with other members of Parliament as part of the Transatlantic Policy Network series of discussions, meetings with the government and counterparts on the Hill.

What are you talking about and what are the issues? What are you saying to people about events and the state of affairs?

MS. IN 'T VELD: Well, I think the particular group that I am part of this week, because there are many groups from the European Parliament visiting, but this particular delegation has been discussing data protection and security issues mainly. It's a bit of immigration and visa liberalization, as well. But clearly, very high on the agenda, usually the first topic that people address are indeed the transatlantic relations and in particular in light of the let's say unusual statements of President Trump in the last week; also before, but in particular in the last week when he was in Europe. And I think his statements have, of course, caused a lot of unease and indignation also in the United States and I would say it left the Europeans more perplexed than anything else. We're not quite sure how to respond to this.

But I think one thing is clear and that is the transatlantic relations, they're very good, they're very solid, resilient. But I think we're also looking at a bit of a reset, and that has to do with changing geopolitics, but it also has to do with changes inside the European Union, the evolution, the further integration of the European Union. And I think in a way it is healthy for the European Union to be a little bit more on its own and we have to take a bit more responsibility for ourselves and for our position in the world.

MR. KERRY: So you've been sort of an equal opportunity critic of government surveillance and by that I mean that you've certainly been critical, as I mentioned, of U.S. surveillance, but also of surveillance by European governments.

MS. IN 'T VELD: Oh, yes.

MR. KERRY: I think you sued the United States. But you're now in a lawsuit with the French government.

MS. IN 'T VELD: Yes.

MR. KERRY: Can you talk about that, what that's about and where that is?

MS. IN 'T VELD: Yes. Well, I just got a ruling a couple of weeks ago which was

negative, which was not totally unexpected, so we're now going to take it to a higher level, to the Human Rights Courts in Strasbourg because we're let's say opposed in principle to surveillance, but it has to be proportionate and necessary, as we say in the European Union. And I think the French surveillance law is disproportionate. And what's even more interesting is that the law goes back to 2015, but it was discovered that in the period from 2008 to 2015, the French government, or rather the secret services, were carrying out blanket surveillance without any legal base. So I've challenged that, as well.

Because I as a member of the European Parliament we meet in France, in Strasbourg, once a month. So, you know, I could theoretically also be in their records somewhere and I want to know. So that's one of the reasons I went to court. But interestingly, they had a very intricate legal reasoning why they could say nothing about that past period, saying because that's the past. Yes, but all the data that were collected during those seven years are still stored somewhere. They can still be used.

But it's an interesting case and I kind of enjoy using all the instruments that democracy offers to us to find the right balance between government powers and individual freedoms.

MR. KERRY: So that brings me to a discussion we were having yesterday about those individual freedoms and the role of privacy in those freedoms. You know, people sometimes see the United States and Europe as kind of Venus and Mars when it comes to privacy issues. Do you think there are fundamental differences in the way that Europeans and Americans conceive of privacy? What do you think are sort of the underlying the conceptions?

MS. IN 'T VELD: No, fundamental differences I don't think. It's true that often people in Europe think that there is no privacy protection at all in the U.S., which is not true. There's quite an extensive legal toolkit, if you want, of protections, but it has a different starting point for European citizens, privacy protection and data protection, which are two different things, but they are fundamental rights. They're on the par with, you know, the right to life, ban

on slavery, and all the other fundamental rights that we have, freedom of speech, equal treatment, and all the rest of it. It is a legal right, it's legally enforceable. And it's not something -- I mean, you have to, of course, accommodate it in certain ways, but it's not, as people sometimes think, a right that you can -- there can be no trade-off with other purposes, like economic purposes or even security. They have to be accommodated. So I think that is different.

And maybe it also has something to do with the history of the European continent. I think we have some bad experiences with governments knowing everything about citizens, in particular in the former Communist dictatorships. And I often sense that in particular my older colleagues from the Central and Eastern European countries who had firsthand experience of what that means, you know, they tend to be a little diffident about surveillance systems. They don't immediately get the feeling that they're safer because of it because they have bad memories. So I think that all plays a role.

In essence, I think the desire that we all have, we Europeans and I'm sure Americans, as well, to be protected against too much intrusion, whether it's by governments or companies, abuse of our data, data that are not adequately protected, I don't think that there's a fundamental difference there between Americans and Europeans.

MR. KERRY: So that brings us to the Privacy Shield. That's a major topic certainly this week of your discussions as the U.S. and the EU go into the second annual review process of the Privacy Shield. The European Parliament, I think you were a leader in this, just voted to call on the Commission to suspend the Privacy Shield agreement. That's something that took place on July 4th. And I'm not sure that was entirely accidental because I also recall that in 2013, when I was still in the government, in the wake of the Snowden affair the European Parliament voted to condemn U.S. surveillance and called on the Commission to suspend the Safe Harbor Agreement that preceded Privacy Shield also on July 4th. (Laughter)

MS. IN 'T VELD: I think that's (inaudible).

MR. KERRY: So is there a deliberate irony in the scheduling of those votes?

MS. IN 'T VELD: No, I don't think we picked the date deliberately. No, I noticed that when people realized what date it was that they thought it was funny.

No, but the thing is Safe Harbor was suspended -- well, not suspended, it was actually cancelled by the courts after repeated calls from the European Parliament to the European Commission to do this because for years we had been very critical. There had been two evaluation reports by -- there was an external evaluation that was very critical of Safe Harbor itself and the implementation.

Those critical reports were somehow, I don't know, put in a drawer by the European Commission. They disappeared, they weren't visible on the Internet anymore. And the Commission just stubbornly refused to repeal Safe Harbor and replace it with something better.

So then the European Court of Justice annulled basically Safe Harbor. Then there was kind of a grace period for companies where the data protection authorities said, okay, we're not going to enforce because that's not reasonable because it's not -- you know, the companies are not to blame. And then they put in place Privacy Shield.

Now, it has been challenged. Like Safe Harbor, it has been challenged in court. I don't know exactly when the court will rule and I don't know how it will rule, but we have very, very strong concerns about the substance of Privacy Shield. We feel that it's still not legally sound.

And the second issue is, of course, even if it's -- you know, whether it's legally sound or not, is the implementation. And there we feel that the implementation is not adequate, which I think is a shame because it's been in place for, what, a year and a half now I believe, almost two years. I mean, ample time to fulfill all the criteria, I would say.

MR. KERRY: And what is it about the implementation that you think is not adequate?

MS. IN 'T VELD: Well, you know, there's the issue of oversight, for example. There's the ombudsman, which still has not been -- there's no definitive ombudsman which has been appointed. Now, they tell us, okay, this is an acting ombudsman, which is just as good. Okay, but then I don't understand why in two years' time you can't appoint somebody, you know, make a final appointment. The people of the Privacy and Civil Liberties Oversight Board, which has not had its quorum for the whole last period, now three persons have been nominated, three Republican candidates, I believe.

MR. KERRY: One Democrat.

MS. IN 'T VELD: And there's one Democrat. Yeah. And so then there's still a vacancy, so they cannot operate. So it's that kind of thing. So it's not even something very complicated and it's just very difficult to understand why even the simplest terms of the agreement cannot be applied.

And then, of course, there's the issue of what's called Section 702, which was basically extended for another six years. It was even widened a little bit, and that was one of the points of concern. So, you know, we thought why was that necessary? And why wasn't it possible to, for example, include what is now the presidential Policy Directive Number 28, which for us, a presidential policy directive sounds like something really funny. Like it's not a proper law. It can be repealed, you know, on arbitrary grounds at any given moment.

Now, the administration told us, yes, yes, but that's all theoretical because it's being applied, you know. It's been so engrained in the system now, it cannot be repealed.

But quite frankly, if I look at the current President, I don't know. I somehow don't feel entirely reassured. I mean, you know, call me paranoid, but I just don't feel that that is sufficient. And I also don't understand why. If it's already so solid, then why can it not simply be transferred into -- or transposed into a law? So it all gives us the impression that the political will is actually not there to really fully ground all the safeguards.

And then again, there is, of course, still the issue that we feel it is not 100

percent compliant with the court ruling on Safe Harbor.

MR. KERRY: So what responses have you gotten from the U.S. Government on these issues this week?

MS. IN 'T VELD: Well, in summary, that we shouldn't worry, that everything's fine. No, in fairness, without being cynical, they are making an effort to implement large parts of the Privacy Shield terms, but there are still these points of concern which have not been met. So it's not that they're not doing anything at all, that's not what I'm saying. But we are still critical of a number of points that have to be addressed, I think.

MR. KERRY: Yeah. So one of the things that's changed since the last annual review is that the General Data Protection Regulation, the GDPR, has taken effect. And it seems to me that for most of the companies that are transferring data to the U.S. under the Privacy Shield that they are subject to the GDPR. So that being the case, what difference do the protections of the Privacy Shield make now that GDPR is in place?

MS. IN 'T VELD: Well, I think they will make a difference because GDPR is essentially about what they do in Europe. This is about data being transferred outside Europe and they may also be used by the authorities, for example.

MR. KERRY: Why do they stop being subject to the GDPR if the data is transferred out of Europe?

MS. IN 'T VELD: Well, it all depends on the purpose. And this is part of GDPR, right? Because Privacy Shield is essentially an adequacy finding, as we call it, saying, okay, data being transferred to another country which does not have a GDPR, but it should have something which is adequate, an adequate level of data protection, or, as the court said, it has to be essentially equivalent to the European system. So that is part of the GDPR logic, but it's no longer literally under GDPR.

Now, I have -- again, the adequacy finding is an instrument foreseen in the GDPR, so we support that. We just feel that the adequacy decision that was taken by the

European Commission, you know, is unjustified. That's the only point.

MR. KERRY: Yeah.

MS. IN 'T VELD: And also, this is about data being transferred which can then also be used by the authorities, which is, of course, another area.

MR. KERRY: Mm-hmm. But yeah, I think my point is under GDPR you need Privacy Shield as a legal basis to transfer the data to the United States still. But in terms of the level of protection that the companies provide to that data when it's in the United States, now GDPR travels with the data.

MS. IN 'T VELD: To a large extent, yes.

MR. KERRY: Yeah.

MS. IN 'T VELD: But I don't think -- that is not the part that we're worried about. And this is also where, for example, the FTC is overseeing compliance by the companies, if they're living up to that part.

But that actually also brings me to another point of concern about implementation or application. Facebook and Cambridge Analytica used Privacy Shield and its predecessor Safe Harbor to transfer data to the United States to be used for the purposes that we now know. And then I think, you know, Safe Harbor existed before. It was faulty, yes, but it was there. We now have Privacy Shield. I believe it's faulty, but it's there and it should be applied.

How is it possible that already back in 2016, the media reported about what Cambridge Analytica and Facebook were doing, and maybe they didn't know every detail yet, but why is it that then the authorities didn't respond? Why was there no investigation? I mean, they're investigating now, but it could have been done much earlier. So that also gives us a feeling.

So, you know, how thorough are they? What does this bring in practice?

MR. KERRY: Mm-hmm. So let's switch gears a little bit and talk about another

issue on which you've been critical of U.S. law. That's the CLOUD Act, the legislation designed to allow extra territorial access to data under our Electronic Communications Privacy Act. This was coming out of the Microsoft case and the Microsoft warrant in Ireland.

You've been critical of that. Why?

MS. IN 'T VELD: Well, to be perfectly clear, and this applies to a lot of different files, yes, I'm very often critical of U.S. policies, but I'm 10 times more critical of the way that the European Commission is protecting and applying European laws, just to be clear.

But why am I critical? Because, I mean, this means, from my perspective as a European citizen, that the authorities of a third country that I am not a citizen of and where I do not have any established rights and where I have no voting rights, that that third country can get access to my data and I have very -- I mean, hardly any means of legal redress. I mean, it's also about psychology because people say, oh, you know, stop, this is the United States. It's a civilized country. They're our best friends and allies. You know, you can trust them.

But if you use a different example, say Russia were to do the same, say Russia adopts a Russian CLOUD Act that allows it, through the Google office in Moscow -- I'm pretty sure Google has an office in Moscow, as well -- and they go to Google in Moscow and say bring us all the data that you've stored in the U.S. I don't think the American government would like that, you know.

And the same goes for China. China is a big country and even if initially -- I'm sure that if they were to adopt such a law, then the Americans and the Europeans would say, well, hang on a bit, you know. There's a limit, you can't do this. But they're a huge -- they're an economic superpower by now. They've got a lot of economic weight to throw about.

So, you know, I don't feel comfortable with this. And I also don't think -- first of all, it's not necessary because we have instruments.

Secondly, if you adopt such a law, then I think it should be done in a proper democratic procedure. That was not the case here. It was adopted on the back of, what's it

called, an omnibus package or something. Something else, in any case. And then you do it also -- I mean, if we are friends and allies, I don't really see why this cannot be done, you know, in a joint process, why we cannot talk about these things together.

And I also think if you adopt this kind of legislation, any kind of legislation giving more powers to the law enforcement and security authorities, then at the same time you also have to strengthen citizens' rights. What I see is that a lot of legislation has been passed over the last let's say 15, 20 years which, first of all, gives more powers to the authorities. And secondly, it gives legal backing, legal protection to companies. And I don't disagree with those two things.

But citizens are increasingly left out in the cold on their own. They're up against the authorities that have massive powers.

I have to say, one of the things, I'm very critical of the U.S. often, but one of the things where I really, really envy you is your FOIA system. That is really something that we should have in Europe. We have something similar, but it's incredibly weak and cumbersome. It's not really -- I've litigated on that, as well, a couple of times.

So, you know, for example, we should have -- if you have more powers for authorities, then you also need a stronger FOIA. You need stronger legal safeguards. It's a matter of balance. Because in my view, and call me naïve or primitive or something, but in my view the state still works for the citizens and not the other way around. And citizens should be able to control the state, the authorities, and not the other way around.

And yes, we give powers to the authorities, for example, to keep us safe, but in a democracy, the essence of democracy is the powers are never unlimited and unchecked. And that is increasingly happening.

So it's all a matter -- it's not a matter of saying yes or no, for example, to surveillance powers or something like the U.S. CLOUD Act. It's all a matter of proportionality and giving proper protections, really enabling citizens to defend themselves against abuse of

power or excess of power or things like that.

MR. KERRY: Yeah. But why doesn't the CLOUD Act provide the opportunity for that sort of joint discussion about legal standards that you talked about? I mean, it provides for international agreements, for reciprocal rights, says that those international agreements must have basic rule of law protections, and that transnational evidence requests need to be based on reasonable justification, articulable, and credible facts, particularity, legality, a lot of the standards that I think are analogous to necessity and proportionality, and subject to oversight by a court judge or other independent authority. Isn't that helping to raise the bar of legal standards?

MS. IN 'T VELD: I'm not saying -- no.

MR. KERRY: And isn't the e-evidence on the EU side having the same effect? Isn't that a basis on which to have that conversation across the Atlantic?

MS. IN 'T VELD: I think it's good that you call it the e-evidence proposal because that's what it is, a proposal and Parliament still has to debate it and process it and adopt a position. Then we have to negotiate with the Council, which is the member states of the European Union, and then there may be an e-evidence proposal. But it all has to do with, you know, as a citizen of a member state of the European Union and as an EU citizen I have certain rights, which I do not have as a non-U.S. citizen.

And I keep using the same example to make it more -- you know, to visualize it. If this were about Russia or China doing the same, you know, even if there are all the same safeguards in their laws, I still don't have the same standing. I don't have the same rights.

And there's a second point, that is that, okay, let's say that a warrant is issued here in the U.S. obliging a company that has stored data in the European Union to hand over those data to the U.S. authorities. The data stored in the European Union are covered by the EU GDPR and probably other laws, as well. So then the company has to decide am I going to comply with the U.S. warrant or am I going to comply with the EU GDPR? Tough one. And in

some cases, I mean, they may contest, that's also foreseen. They may contest the warrant. But citizens' rights cannot depend on the choice of a company, you know, whether to comply with a court order with the GDPR. I mean, that means that I am completely at the mercy, if you want, it is completely arbitrary. So I think that is really something that needs to be redressed.

And then thirdly, within the European Union, if we get something like e-evidence and we have similar instruments or let's say related instruments like the European arrest warrant, like the evidence warrant, like investigation order, stuff like that, but that is all based on a system of cooperation, mutual recognition, common European standard, common European rights. Because I as an EU citizen, I have the same rights no matter where I go in the European Union and I know I can exercise those rights. So it puts me in a very different position if, let's say, the court's order issued in, I don't know, Hungary retrieving my data in the Netherlands are then transferred. It puts me in a very different position.

But there are some question marks there, too, because we have a situation at the moment whereby there are some so-called judicial reforms in Poland which we believe have led to a situation whereby the judiciary can no longer be considered independent. This is not my political view. This has been established by all sorts of independent bodies.

Okay. And there's even an official procedure that has been launched by the European Commission against Poland. So that makes it complicated because let's say that it is a Polish court or a Polish authority issuing such a warrant. Then, you know, what's the situation then? Should we recognize that or not? Is it then for the company concerned to say, no, you know, we're not going to comply with the warrant because it's been issued by the Polish authorities? I mean, so there are some questions that we need to answer inside the European Union, as well.

MR. KERRY: Yeah. But under today's law, if the U.S. Government is investigating you and gets today's -- before the CLOUD Act, gets a warrant and goes to the Dutch government under Mutual Legal Assistance Treaty, is there any process in the

Netherlands to decide whether that's a valid warrant under European law? Don't they simply accept, okay, we have a valid order issued by a judge in the United States? We have an obligation under the MLAT to effectuate the production of the evidence, we'll do that. And what opportunity would you have to, A: find out that you're under investigation and object --

MS. IN 'T VELD: No, but I could still -- but there's still --

MR. KERRY: -- to the production of that evidence?

MS. IN 'T VELD: Yeah, but the point is that the Dutch judge in this case would still be part of the democratic system in the state that I'm a citizen of and where I can exercise my --

MR. KERRY: What Dutch judge?

MS. IN 'T VELD: What do you mean what Dutch judge?

MR. KERRY: Is there a right MLAT to have a review by a Dutch judge or is the process carried out by the government?

MS. IN 'T VELD: No, I can exercise my rights. I can challenge decisions in the Dutch system, which is a lot more difficult, not to say impossible, under -- I mean, I cannot as a Dutch citizen -- yes, I have opportunities. Yes, you can litigate in the United States, but it's a lot less certain, it's a lot more complicated. People need to be covered by their own laws and not laws of a third country.

Are the MLATs -- do they need to be improved? Yes, I think everybody agrees on that, not least because the whole procedure is very cumbersome. And this is one of the reasons that authorities are trying to find a way around it, simply because it takes too long.

Now, I think we should focus first of all on improving the MLATs. And then, if then there's still gaps somewhere, then we need to find other solutions. But those solutions are supposed to be adopted in a proper, open, democratic procedure. And if it concerns, for example, my rights as an EU citizen, then I want to have a say over it. And I think that's only fair.

And if we are friends and allies, then I think we should be able to find processes to ensure the protection of rights of each other's citizens. You know, progress has been made in this area. There's the Judicial Redress Act, but that is not 100 percent watertight. But it's definitely a step forward, but there have to be rights because under the Judicial Redress Act certain rights can be repealed unilaterally by the U.S., which means that they're not actually a right and it's something which is granted to me, a kind of favor.

So I think if we allow authorities in the U.S. and in the EU in this case to exercise power over -- we over your citizens, you over our citizens, then the rights should also be guaranteed equally on both sides of the Atlantic. And that is simply not the case yet. We have, of course, a system which has a slightly different philosophy whereby everybody in the European Union is covered by the same laws. We don't have rights on the basis of nationality. You know, if you're covered, for example, by European laws or the European Charter of Fundamental Rights, it applies to everybody. So it's a different approach.

MR. KERRY: Well, let's move the conversation out to the audience. I invite your questions. I think we have a microphone in the back of the room, so please wait for the microphone to get to you. And when you ask your question if you can stand just so everybody can see you and be sure to hear you, and if you could identify yourself.

Sir, on the aisle here.

MR. SHONANDER: So thank you. Thank you, Ms. in 't Veld. My name is Carl Shonander. I'm with the Software and Information Industry Association. And thanks for acknowledging the Judicial Redress Act. That's something that a number of us worked a lot on a couple of years ago.

Two questions. On Privacy Shield you talked a lot about implementation and I think we're familiar with the issues there. You also mentioned something about that the legal basis was not sufficient. I'm not really I understood what you meant by that, so I wondered if you could elaborate on that.

And then my second question is, after this discussion on the CLOUD Act, so I take it you would not support either individual member state law enforcement sharing agreements with the United States per the CLOUD Act or, as the European Commission wants, an EU-U.S. law enforcement sharing agreement per the CLOUD Act? Thanks.

MS. IN 'T VELD: Well, on the first question, it's not so much that there's no legal base. The question is, is Privacy Shield compliant with the criteria set by the European Court of Justice in its ruling on Safe Harbor? Because it set certain norms, if you want, and I believe and some people who've challenged Privacy Shield also believe that it's not fully compliant.

Give you a small example. The courts are actually across a number of rulings, by the way, they're opposed to let's say the blanket, indiscriminate collection of personal data and long-term storage. Let's say the bulk collection of data. And they say it has to be targeted. Now, this is, amongst other things, in the Section 702. And indeed, there is talk of targeted surveillance, but the definition of "targeted" is a different one than we are using. And it could be, for example, targeted that could cover a particular period of time or a particular area, which, in our view, is still bulk collection of data. So that's one of the things.

Another question is whether indeed the presidential policy directive can be seen as an adequate legal protection or if that's too flimsy. I mean, there's that kind of questions. So it's not so much about legal base, but about whether it complies with the court ruling on Safe Harbor.

On the U.S. CLOUD Act, would I consent to bilateral agreements between member states and the U.S.? Well, first of all, it's not for me because I'm a member of the European Parliament, so I don't get to vote on national laws. But as a rule, you know, in any policy area I don't like that instrument of 28 bilateral deals with the United States. I don't think it's in anybody's interest. It's not workable. I don't like it.

Will I agree to a European agreement? Well, that remains very much to be

seen. That all depends very much on the terms and conditions.

In any case, I would never consent to something which has been negotiated -- or which has not been adopted in let's say in open and democratic parliamentary procedure. I think that's really the very first condition for consenting to anything.

MR. KERRY: Additional questions? Ma'am?

MS. BRUNNER: Thank you. Lisl Brunner. Thanks for coming and speaking to us. It's a really interesting discussion.

Following up on your point about equivalences on both sides of the Atlantic, what is the equivalent of PPD-28 on the European side? And I noticed, it was very interesting, that as the EU was negotiating with Japan to form an adequacy agreement, Japan, despite its incredibly strict data protection law, had to meet some extra steps, had to take some extra measures in order to qualify. And one of those was that EU citizens had to have a remedy against the Japanese government. Do Japanese citizens also have an effective remedy? Do U.S. persons have an effective remedy in Europe and what does that look like?

MS. IN 'T VELD: Well, they're are two questions essentially. Do we have something like a presidential policy directive? Certainly not at the European level because we have a completely different constitutional arrangement, if you want. Does it exist in countries like, I don't know, France? Maybe, I don't know. But we have 28 different member states with different legal and constitutional traditions, so that I cannot say, but certainly not at the European level.

Any legal act or law would have to pass the proper parliamentary procedure. It would have to be negotiated with the other legislative branch, which is the Council, which is the 28 member states.

And then on do Japanese and U.S. persons, for example, do they have the same rights to a legal remedy in Europe? Yes, because, again, they're all covered by -- we don't have European rights and laws apply to everybody in Europe. For example, there are lots

of people living in Europe, not just citizens from other countries, like the U.S. and Japan. But even stateless people who are living in the former Communist states and who lost their nationality in the whole process when they fell out of the Soviet Union, and so they don't have any nationality at all, but they're still covered by EU rights.

MS. BRUNNER: And so why is a U.S. person trying to challenge the European governments' access to my data in the way a European person could perhaps (off mic)?

MS. IN 'T VELD: Yes, you can -- under, for example, the GDPR or other pieces of data protection law you can go can go to court, sure.

MR. KERRY: So I guess to elaborate the question, though, it seems to me that for many years the norm in government surveillance internationally has been we may have certain protections for our own citizens, more or less, depending on the country. But outside our country anything goes. And certainly as a traveling official, my security briefings always said assume in any country you go, and this includes European countries, that you are under surveillance. And that anyplace you go, anything you say, and your communications may be picked up.

PPD-28 does set a new international norm and says we are going to extend equivalent protections to the non-U.S. persons who've been subject to that anything goes rule. And I think the question goes to, to what extent has that norm been followed by the European states or other countries?

MS. IN 'T VELD: I'm not sure that we followed PPD-28. But, no, as I said, our whole system is based on a different assumption. It's not based on, you know, nationality.

But I think in the end, because you rightfully say that intelligence, security, law enforcement forces, they work across borders. They're sharing information. In particular the intelligence community, they're sharing information the whole time and they're actually sometimes even trying to circumvent what you say, that they cannot spy on their own citizens by asking the intelligence services in a neighboring country to spy on our citizens and the other way

around. And then they swap, kind of.

And I think that means that rights of citizens, and also if you're not just looking at the authorities and surveillance, but also what companies do with our data, I think it is high time that we should have some sort of global standards. And I head that after the whole Facebook-Cambridge Analytica scandal, which was a very clear example of why private protection is not only a right of the individual, but why it's also essential for protecting our democracies, people in the U.S. also said, you know, hang on, we also want something -- we want our own GDPR-like law. I understand a law has been passed in California which is very close.

I think it's all a matter of if you create powers on one side, then you also have to create the protections on the other side. And if powers, whether it's powers of the authorities or powers of big companies, if they extend across borders, then so should the protections and the rights of citizens.

And I'm pretty confident. I'm an optimistic. Otherwise, I wouldn't be in politics. So I always believe that we can make things better and change them. And I think this will happen. It will evolve. Because when I first started to work on privacy issues, which is about 15 years ago, people at best thought that I was a harmless fool and at worst that I was either going to kill industry or security or both. But today, nobody is questioning the importance of privacy protection anymore.

I mean, and you can see that even companies like Facebook or Google, even if they do everything they can to abuse our data because that's part of their business and it's legitimate, that's what businesses do, but they're increasingly talking about privacy and protecting our data because they realize it's important to people. They realize it's important to their customers, just as 10 years ago -- you know, 20 years ago, if somebody wanted to sell a car, a manufacturer, he would say this is a great car. It can speed and it's big and it gives you status and it's whatever, great car. But that has evolved. If you want to sell a car now you have to say it is environment-friendly, it has low consumption, low emissions. That has to be part of

the sales strategy.

And the same is happening, I think, with privacy. Ten years ago, everybody said, yeah, yeah, you and privacy. Now everybody realizes it's important. And the fact that companies like Facebook and Google are trying to convince their customers that they care about the privacy of their customers means that they realize this is necessary to keep their customers on board. And it may well be.

And I also think that when it comes to privacy, there are -- okay, we have privacy laws and that's a very important tool for ensuring our privacy. But there are other tools. One is competition laws, which is a very, very important tool I think for making -- you know, forcing companies to take our privacy more seriously. If there is now a company which is really privacy-friendly, it really has a competitive advantage. Competition law can, of course, also be used against monopolies that are using our data.

And the second element is we need to let's say monetize the value of personal data, not just to provide incentives and disincentives to, for example, companies, but also if you -- for example, the whole PNR thing and SWIFT and storing of data, and more and more companies are actually being obliged by the law to store and process and provide personal data to law enforcement and security authorities, okay, there is a cost to that. It doesn't come for free. And the cost very often is born by the companies, which, in a way, is not fair because they are carrying out a public task.

Now, if the same cost had to be borne by those authorities who want those data, it would appear in the national budget. And then every year politicians would have to explain why they want to spend money on surveillance and on the collection of personal data and not on, I don't know, education, healthcare, new roads, whatever. And then it becomes political and more democratic.

So I think expressing or sort of putting a price tag to personal data and a price tag to the use of personal data, whether it's by companies or by authorities, is also going to

change privacy protection I think.

MR. KERRY: Well, maybe we'll get to a baseline federal law in the United States. I'll put in a plug for the paper that I put out, a Brookings paper on privacy last week.

So we've got time for about one more question. Over here on the right, my right.

SPEAKER: Hi, my name's Wendy. I'm a sociologist at the University of Wisconsin.

You mentioned earlier that there are many ways that we can address the privacy issue through domestic laws, competition laws, and we've also been talking a lot about surveillance, but, increasingly, this issue has been taken up in trade agreements. And so I'm wondering what do you see as the path forward and dealing with data flows and the free flow of cross-border data flows in trade agreements? And how has the EU conceptualized this with, you know, recent trade agreements in Canada, Japan, and maybe going forward the U.S.?

MS. IN 'T VELD: Okay, I'm not an expert on trade agreements, but in principle there's been a kind of carve-out for that, which is -- well, in a way that's a bit forced or artificial because clearly it's a very important part of trade. And probably, again, you know, I'm not an expert on trade agreements, but I'm sure that they will become part of future agreements. But then first there needs to be a proper basis, you know, that we need to know that our trading partners are going to respect the same rules.

And again, I also think that, look, the GDPR didn't come from nothing. We had, for 23 years, we had a Data Protection Directive which contained a lot of provisions that are also contained in the GDPR. And that's not, you know, prevented trade from happening.

And it's also forced somehow companies to adjust their strategies. And I think the GDPR will also become some sort of global standards and industry will have an interest, like with the directive, which is also, you know, a standard which is being increasingly applied in other countries. They will have an interest, a commercial interest, in global standards. And as

the directive bit by bit became a global standard, or at least something that was a model, I think the GDPR will also become a global standard. And it's actually going to make our -- it's going to protect our privacy, but I also believe it's going to make our industry more competitive and more innovative, as well.

MR. KERRY: Let's try to squeeze in one more question. I think over here on the left. Yes, sir, right in front. Make the question short and a short answer.

MR. URBIOLA: Yes. A very short question. I'm Pablo Urbiola from the Institute for International Finance and a new citizen.

You were mentioning that in the European Union privacy and data protection are considered fundamental rights. So should the EU promote global debate on data protection, to have international standards as we have for other fundamental rights? Because otherwise, we might end up in a situation with very different regulations across the world and problems for the digital economy, for the use of cloud computing, for international trade based in database services. So why not go back to a discussion on the principles?

MS. IN 'T VELD: No, I fully agree and that's not being done sufficiently. We're promoting all sorts of human rights or fundamental rights or citizens' rights, but this one we don't promote it very strongly. And sometimes that leads to a very cynical situation.

One of the things that I find very difficult to stomach, for example, is that as part of the new immigration strategy, we're giving money to all sorts of governments, not necessarily shining beacons of democracy and rule of law and fundamental rights. And we're paying them money to set up systems to register their citizens, border controls, you know, storing biometrics. And some of those countries are actually dictatorships. So, you know, I find that very difficult to accept for a number of reasons, but this is one. Why don't we apply the same standards? If we believe that this is a really a fundamental right, then that is a right that should apply to every single person on this Earth and not just to us. So I agree.

MR. KERRY: Well, we need to wrap it up. Quickly, next year's an election year

in the European Union. Any prognostications before we go? (Laughter)

MS. IN 'T VELD: No, no, no. You know, a week is a long time in politics and 10 months is certainly a long time. But it is a very exciting time. A lot is happening. You know, and we have a saying in Dutch that under pressure everything becomes fluid. And that is sometimes scary, but it's also the moment where you can actually give things a different shape. So it's very exciting.

MR. KERRY: Well, Sophie in 't Veld, thank you very much. You've been outspoken as promised.

MS. IN 'T VELD: Thank you for having me. (Applause)

* * * * *

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