THE BROOKINGS INSTITUTION

SAUL/ZILKHA ROOM

THE FUTURE OF EU DATA PROTECTION: A VIEW FROM A LEADER IN PARLIAMENT

Washington, D.C.

Thursday, March 29, 2018

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

BIRGIT SIPPEL
Member and Rapporteur for the e-Privacy Regulation
European Parliament

* * * * *

P R O C E E D I N G S

MR. KERRY: Good morning everybody. I'm Cameron Kerry. I'm the Ann and Andrew Tisch distinguished visiting fellow here at Brookings in the Governance Studies program. I want to welcome all of you this morning to this discussion about the e-privacy regulation in the EU. I encourage everybody to Tweet with the hashtag that's up there on the screen but please be sure to silence your cellphones. We will have questions at the end of this so keep those in mind. When we do get to the questioning, I ask that you stand up and identify yourselves and we'll have somebody come around with a microphone.

Many people have heard about the General Data Protection Regulation in the EU. With recent events, there has been a lot of awareness that Europe has this new broad privacy regulation coming into effect on May 25th. There has been much less attentions operated a little bit under the radar on the e-privacy regulation which was intended originally to be done in time to take effect May 25th but it has taken a little longer.

So we have the right person here to talk about that, Brigit Sippel. She's a member of parliament at the European Union since 2009 coming from Germany. She is a member of the social democratic party in Germany and of the socialists and democrat group in the European Parliament. She is a leader of that group within the LIBE Committee that oversees particularly data protection issues. It is the equivalent roughly of being a ranking member. In particular, she is the manager for the LIBE Committee for the e-privacy regulation. She is taking that docket into the process of negotiations with the European Council. So with that, let

me turn to Brigit Sippel and ask you to set the stage a little bit.

I mentioned there is General Data Protection Regulation taking effect, it is comprehensive. It covers all sectors in pretty comprehensive detail. So why an e-privacy regulation? Why is there a need for a special law to address electronic communications?

MS. SIPPEL: Okay thank for that question. First of all, thanks for inviting me and having this opportunity to talk to and maybe with a lot of people here in the United States. During the IAPP conference, I got aware that, of course, the GDPR, the General Data Protection Regulation, has got a lot of awareness because there are a lot of detailed rules within that legislative file. And also, of course, the interest here in the United States is big and also in other areas as we decided that that regulation should apply to everybody doing business and services in the EU for people staying in the EU. So a lot of work, I could imagine, already has been done to clarify or what can we do to apply to that rule. So why, in addition, an e-privacy regulation.

We had some debates in the European Union. If it wouldn't be have been a good idea to have both the data protection and, in addition, the e-privacy, trying to do it within one legislative file. But the history of both files is we have different legislative files so we are continuing the process. The reason why we have the e-privacy regulation is that in coming from the European Union for us, privacy and data protection, they are fundamental rights. In addition to some rules, how to process data, what can you do, what can you not do with all the different kind of data, the question of protecting privacy, your private like if something where you

have to get some more attention. Some strict rules, how to ensure that we stop this. I personally call it digging into my privacy as digging into a gold field without any respect for my personality and private life.

So that's why we started to work on this e-privacy regulation that will apply, same like the data protection regulation, to all companies offering goods and services to people within the EU. So it seemed to be a very easy legislation, just complimenting the data protection regulation but it came out that there is now a big fight that this is the evil legislative thing. But I believe, to some extent, that is because people were not very aware about the rules that already exist. I will only start before we go in to debate with one example. Many people do not understand why suddenly we give so much importance to the principle of consent. But the truth is at least for the European area because it is so far a directive law only within the EU.

So the directive already says since 2009, if you want to track people you do need prior consent. So it is not a new rule but to be honest, very often it has not been completed respected. Of course, those who never respected the rule in the past, don't want to respect it now. But we decided that we need to be more strict on that so a lot of debate is around that question. By the way, of course, consent is good but it is not there in all areas. And consent, of course, coming back to the General Data Protection Regulation, everything that is illegal according to the General Data Protection Regulation will continue to be illegal even is you ask for consent because you can't give consent to something that is illegal.

MR. KERRY: I'm still puzzled because the General Data Protection

Regulation, I mean, you talked about digging into privacy, my privacy, to tracking. The General Data Protection Regulation has provisions dealing with profiling with additional consent required for profiling and a number of provisions affecting marketing. So what is different? What is the added problem that you are trying to address?

MS. SIPPEL: Okay with the General Data Protection Regulation, we are talking about data you might have gotten from different areas by different means. With the e-privacy regulation, we precisely talk about communication. So all communication data, if it is emails, SMS, WhatsApp's and Skype. So whenever there is a communication, that communication needs to be very strictly confidential protected. So it's not the data themselves but the communication that needs to be respected. In the European Union so far, with the current directive, we have protected emails, we have protected SMS messages. But everything that popped up after the old current directive, so-called over the top services like WhatsApp's messenger, Skype and other things, those forms of communications are not protected because they haven't been there when we decided the old directive.

So for us it is very clear, communication needs to be confidential and protected. There shouldn't be a difference if you send very old fashioned, I do not know if anybody is still doing it. If you send a letter, a paper letter into an envelope, give it to the post, send it, that letter, of course, should be confidential. If I send you a letter only you should read it and nobody in between. So the same thing should go for phone calls, phones messengers and everything else. So that's the additional thing more precisely to every that's in communication.

MR. KERRY: Talk a little bit about metadata. Because certainly in the analogy that you've talked about and the contents of the envelop are sealed. But the postal service and potentially other people can see and in some cases need to see the address information on the front and at least have the potential to see the return address if it's on the envelope. The equivalent in the electronics communications if metadata, the addressing information. The detailed records in the case of phone companies, email addresses or URL's in the case of other online communications. How does the regulation treat those?

MS. SIPPEL: First of all, we are only talking about letters and the equivalent would be an SMS or an email. Of course, you need to know where the communication starts and where it should end. But here the first point is the postal service needs to know where should I send this letter but the postal service shouldn't give that information. Oh here, I have a letter from Brigit to Kerry, how often are they exchanging letters. I should look upon it, postal service shouldn't do that. They just send the letter and then forget about the data. The same should be for others.

In addition, we are talking about communication via the internet. You are not only phoning a company to order, old fashioned example, a book, you go to an internet page and say hey, I would like to buy a book. The problem is that yes, of course, the service provider needs to know your name, address, credit card so that you can do the pay for the book. But is that service provider allowed to take that data and link it to other information the get of you or are they allowed to sell the data to others. So inform other companies, hey Brigit Sippel has bought ten books. Maybe she's interested because the books are all about how to prepare your garden

better so she might be interested in a winter garden or something like that. So they are selling the data to someone giving other services. No. If they want to do that, they have to get my permission. So you see a lot of things are going around. Some metadata are needed for a special service but if you need to do more, you need to consent as long as it's not illegal.

MR. KERRY: I want to explore how some of that data can be used because there is beneficial potential. Take your analogy. You send a letter to me and we probably all agree that keeping track of how many times you are communicating with me is problematic. The postal service may have an interest in knowing how many letters it is delivering to the United States as opposed to other places for purposes of its planning. When it comes to metadata, there is a lot of potentially socially useful information.

I did a paper here at Brookings about three years ago on the use of data for social good. I was actually the co-author of the paper. The lead author was actually a Belgian who was a graduate student I worked with at MIT who is one of the leading scholars of what you can learn from metadata. The person who flagged that, you could take what is supposedly anonymous telephone records and with just four points in time and space, be able to identify one person uniquely. There are certainly privacy issues that that raises. What we were examining in the paper was that there are uses of that metadata that can be socially important. It has been used for disease tracking. So we were looking at these scenarios for using records for social good, for humanitarian purposes and the challenges of doing that while protecting privacy and also the regulatory challenges.

In fact, as we were working on this paper the Ebola crisis happened. There were efforts to try to use telephone call records to help track migrations of population to help look at potential pathways for migration of disease. Can you do that under the privacy regulation? How does it impact the ability of communication service providers to share their data for purposes like that? Those concerns about doing that were part of the things that inhibited the use of that data in the Ebola crisis.

MS. SIPPEL: Okay I would start with the first example to start with the easy thing. Postal services might need to know how many letters are going to and from the United States, how many letters do come in to Washington or are leaving Washington. But for that purpose, you do not need to know who is writing a letter to whom, you need to count the total number of letters. And then you need enough staff to distribute them into the town, that's true, but you don't need exactly who is writing a letter to whom, so that's no problem.

Interestingly enough, we always got these examples. There are very good things you can do with data. The problem today is that collecting different data you can use them in very different ways. We see today with the (inaudible) is not the only example and to be honest not very new to some extent. We had some knowledge it could be done that way with Facebook and Cambridge Analytical. So you can use those data in your example maybe to deal better with health crisis but you also could use the very same data for discrimination, to stop all kind of migration.

So that's why the purpose needs to be described very precise. You need to find out whose data are you collecting. And for those who are preparing the good thing in the health area, do they have the individual data. Is it necessary to

know that Brigit Sippel might have a disease problem for the purpose you are working on. So these are all the questions where we say, if it refers to an individual, then you have to be very, very careful and then it depends is there a noble role public interest. We are talking about legitimate interest, we are very critical on that to broaden that too much. But we do need, in any single case have that definition, is there an overall public interest in that knowledge and how can we then do it while minimizing the risk for the individual to totally give up his or hers privacy.

MR. KERRY: So let's follow up a little bit on legitimate interests you said. You've been critical of that and that has certainly been one of the controversial areas. For those who aren't into the (inaudible) European data protection, the data protection regulation allows data processing of the basis of legitimate interest of the company that is doing the processing or that holds the data. Provided that they balance that interest against the protection of rights of the data subject, the person that the data is about. It is my understanding that, as the Parliament has reported the legislation, that's not allowed under the e-privacy regulation. Do I have that right?

MS. SIPPEL: Coming back to your example of the health risk, to be honest, that's not precisely maybe done under e-privacy but under GDPR. Where we have some rules if a hospital, doctors, have some information and it is necessary to deal with it for the purpose you mentioned, maybe they can use it in an anonymized way for such purposes, but that is data protection. And in e-privacy, we are not only talking about health data, we are talking about communication. I'm communicating with a hospital. Me communicating with a doctor. Me communicating maybe with an

internet page to get some advice and that communication needs to be protected. I don't want my health data in the hands of my employer, for example. Maybe I don't even want that data coming from that communication to be given to family members, I don't like that for different reasons.

So that communication needs to be protected. That's privacy. If the hospital still has the data and there is an overall interest to say suddenly there is a disease risk and it is growing, we have to find out why, then we are in the area of data protection regulation, so that's not a privacy. We have to be very careful in which area we are just dealing.

MR. KERRY: Yeah but let's try to keep it in the context of e-privacy. So take our postal service example. I think what I was saying about using the address information for business planning is that an example of legitimate interest. To put it back in the context of e-privacy, does it allow, my understanding is, it would not allow for processing based on legitimate interest.

MS. SIPPEL: I wonder why we are going into such details and I wonder how have postal services in the past been able to do their service. Without doing all that investigating in private data and privacy data, they were able because they had the overall information. We do get a lot of letters coming to Washington and then they could do it. We have to be very careful. If we are talking about examples that might look nice but maybe do not have that big additional value that really you could consider for that purpose, I need to give up my privacy.

So to that extent, once again, when talking about privacy and my private communication, that's a fundamental right. And you can't balance fundamental rights

against some business interest, commercial interests. You can't say, oh the commercial interest is bigger than the fundamental right. Sometimes you have to find practical solutions, that's true, but you can't balance a fundamental right.

MR. KERRY: Doesn't GDPR do that on legitimate interests where it says balance the legitimate interest with the rights of the data subject.

MS. SIPPEL: Not to the individual. We are talking about general data regulations so once again, coming back to your example. If in a special area, doctors or hospitals get aware that suddenly many people do suffer from cancer or something like that do suffer from cancer or something like that. Then there is, of course, good reason trying to find out could there be a special reason why this is happening. So you have to do some research.

But that research mustn't be on the basis of individuals if you are doing it on the basis of the individual trying to find out where are those persons who suddenly suffer from that disease. Where are they working, what are they doing, what is happening in their gardens, many things can happen. Then you have to contact that person but then you do need their consent, could we please work for that, we have a problem in that area we need to find out. So first, you need consent and second, you need to make sure that these information are really only used to find out what is going on in that health area. You can't give that information to other services doing other things or to other commercial interests.

MR. KERRY: So the other area that I understand has been particularly controversial or the subject of certainly lobbying and debate is the impact of the e-privacy regulation on advertising, electronic communications in media,

particularly online media. Can you talk a little bit about how this regulation effects that area and your thinking behind that?

MS. SIPPEL: That's a big issue also in Europe for the press, for the media, saying with that regulation, that's the end of all of our media services online. And why do they believe that. First of all, there are different things that happened and that can't be solved or better regulated only by e-privacy. The first thing is, when we started with all these nice digital services starting with things like Facebook, Amazon we thought oh those are great things, we can do it. Down streaming films was another thing without any cost. Instead of going to a shop asking for a film paying money, he we can down stream it without any cost. But what we forgot in the very beginning because we all more or less were fascinated of these new possibilities, what we forgot is it is nice that you can down steam, that you get information for free, that someone has to do the work and the work needs to be paid for.

So how we are organizing that and we saw that there are some developments regarding getting films and music for free. Now we organize some services that you can do it via a platform but you have to pay some amount of money.

So with the media, we have a general problem. Even before we started with all these digital newspapers online, many media at least in Germany and in Europe I can talk about the situation in Europe, they already had some problems. And media pluralism already had been under threat before for very different reasons. Because many people thought I don't need a newspaper anymore, I can look at the TV, I can listen to the radio, why should I pay for a newspaper.

That started long before and then with the internet, press media decided oh we go also to the internet but how do we organize it. We make it for free but and that is what has taken place today. And very often, without the readers really knowing about it, you will be tracked. So there will be a platform and the magazine, the press will say oh we are following our readers and we are not only looking how often do you read my newspaper, but they will follow you all over the internet, oh what are my readers doing. Which internet pages do they visit, how often, how long, what are they doing. All these information they create profiles and they sell it to whomever is interested. I'm convinced, many people do not know that this is happening.

This is practice since 2009 and to some extent is illegal, has been illegal. No one really cared about that it might also be a political problem that we did not push enough. But now with GDPR it's not only a privacy, with GDPR we say if you want to track, you need to ask for consent and the consent has to be specific, freely given and informed. Just saying, oh I track you, that's nothing. Who is tracking me for what purpose. It is not specific, it's not informed. So it is already no longer possible and the GDPR is not the e-privacy. The problems for the media to get the money for their work to do to finance journalisms, I'm sorry that problem can't be solved by data protection maybe we need to find new ways. And we already see they try to get money for the newspaper for single articles. Maybe even some newspapers but that is on them to decide by creating a platform altogether so that people are ready to pay a special amount for two or three newspapers and read some of the articles.

So I agree for the media, there are some problems but the problems

started before. The problem with consent does exist even without e-privacy because once again, consent needs to be freely given, informed and specific but that's already in the GDPR.

MR. KERRY: So how should we pay for media? What is your vision of how the media survives in this online world where there is many sources of content and some of the traditional sources of advertising have gone away. Here in the U.S. we have Craigslist has wiped out the classified advertising sections of newspapers.

MS. SIPPEL: First of all, once again, everything we use in the internet at the end going into the detail, there is some work in the end. If it is a journalist, if it is someone producing things, if it is someone writing a book, doing some music, there is someone really working and those people need to be paid. Sometimes I'm asked, hey you want the media that we have to pay for their work if it's in the internet. That's not good because everybody has a right to information even if they are poor people. I don't understand that argument because I can't remember any time in the past where information was for free. You always had to pay for a newspaper and it is true sometimes, poor people workers organized their own newspapers but not because of the money but because they wanted to have different information. So information never has been for free. I think the argument that it has to be for free is simply because people want to make business with the data and we are not only talking about creating a newspaper.

By the way if you ask how could it be done, to be honest, I'm a little bit old fashioned. I like when being home to have my printed newspaper, especially on the

weekend. Take some time, have the paper in the hand, look around, read the one article, read it again, that's fine, but I'm not always at home. As a member of European Parliament, I have to stay in Brussels, I have to stay in Stroudsburg and the digital version of my newspaper I can read it also here in Washington. So I'm paying a special amount for getting my printed newspaper every morning at my home in Germany and paying an additional amount of money to get regularly this digital version of my newspaper. I also pay a special amount of money for a weekly journal that I have in Germany, so I'm ready to pay.

You might say other people do not have the money to pay two or three newspapers but that has nothing to do with e-privacy. Maybe we have to think about the wages that we pay to our people. If you don't have enough money to even pay for one newspaper, the problem is not in e-privacy then the problem is in the wages that we pay.

MR. KERRY: Let's talk a little bit about the model and how that gets affected here. So paying for information, you get a digital subscription, that gets you past a paywall. It's okay to have a paywall. Is it okay to have a tracking wall that says, you can't have access to our content unless you agree to basically allow us to serve ads?

MS. SIPPEL: The question is, what does it mean. Do you allow me to track you. Once again, does the newspaper tell me, I would like to know how often you are reading our newspaper. I would like to know which articles are you especially interested and then I can think about okay, that's my newspaper. Do I trust them and it is good that they try to find out in which areas they should deliver more articles

because I am interested in. But that's not what they really do.

So the other question is, will they ask me and once again, already under GDPR, consent needs to be specific. You have to ask, yes we as the newspaper want to follow you to improve our service, do you agree with that. But we also want to sell your profile with everything you are doing in the internet to others, do you also agree to that. I could imagine not everybody would agree to that for good reason. The fact that people so far are not protesting simply might be that not everybody really is aware of what is going on. So we are simply willing to give back people a little bit of control about their private life. We also have to keep in mind, if you say we are doing it everybody can be tracked, you sell that information so you have a tracking wall, you need to do that.

We could also talk about fake news, what does it mean. If you depend for your newspaper on many clicks so that you can say to the advertising sector, hey a million people are following me so you give me to the money than to another newspaper because the other newspaper, only a 100,000 people are following them. So what does it mean, what will you do to get that many clicks? Will you really work on good journalism, investigative journalism or will you say, oh we also have to work on other things to get all the clicks so that somebody from the commercial area will give me the money. We have to think about that.

MR. KERRY: So let's turn to all of you for questions. Yes sir.

QUESTIONER: My name is (inaudible) I'm here with Morgan Lewis here in Washington. I want to bring in another issue that's a hot button --

MR. KERRY: The microphone is coming although you have a very

booming voice.

QUESTIONER: -- and that's the Cloud Act. You may have heard that last week as part of the Omnibus Budget on page 2,200 there is a Cloud Act in there that basically invalidates the Supreme Court's case right now against Microsoft allowing access to personal data in Europe, stored in Europe through U.S. warrants in case there is such a scenario. The only way to get around that is you can demand a hearing by a Judge but only if you are a qualifying foreign government. I don't know what that is already. Why isn't the EU Parliament all up in arms about that? I think that is a big violation of the Article 48 of the GDPR and others but I don't hear a lot from the EU Parliament on that.

MR. KERRY: Before you answer that, I do want correct aspects of the question. A U.S. provider can also object if the warrant is for the data of a non-U.S. person or if it believes that the request would violate foreign law.

MS. SIPPEL: First of all, I think we hope that this Cloud Act will never come. So we had it on the radar but now it's there last week. It's true, it has been debated some time here in the U.S. This week, I had some debates with representatives from the U.S. Not everybody here is really aware what it practically means.

From the side of the European Parliament, you might know that we supported Microsoft in the Microsoft case where we already talked about the question, is it really necessary or legal or important that they give away data that are stored in European Union. We clearly supported Microsoft in their position to say the data are in Europe, most of the data may be of European citizens or people staying in Europe

so there is no U.S. jurisdiction, we don't want to give away the data.

Now with the Cloud Act, we already contacted our commission to say, we have to check what this means in practical terms. Once again with the Microsoft case, we clearly said no that's against our rules we don't want to give away data, so we are right now starting the process to check into the details.

MR. KERRY: Next question. Yes.

MR. WANGER: Hi, Eric Wanger form Cisco. I want to push a little further on this idea of consent because you said you cannot consent to things that are illegal. If something is not permitted under the GDPR, then you cannot consent to it and this may be the difference between the U.S. law and the law in the E.U. But consent actually here does define, in some ways, the things that are permitted and are not permitted. So if Cam were to come up to me and hit me, he could be criminally prosecuted for that. But if beforehand I were to say to him, please hit me, then he would not be prosecuted for it because it would be within the bounds of my consent.

So I believe that you agree that the reason that things are provided for free is that an exchange for that, that there is some value that's being derived from the tracking of the behavior. I certainly get the idea that the consent has to be specific, informed and freely given. If those things are true, and people do understand because I think it is a fair question whether or not people understand the actual extent of the tracking and therefore the value they are exchanging. But if they really do understand specifically what tracking will take place in exchange for it, is there a role for the government to decide that certain types of tracking are beyond the scope

of what people should be able to consent to. Is it a question of people understanding or are there things that people can't actually agree to?

MS. SIPPEL: So first of all, coming back to that link between GDPR and e-privacy, everything that is illegal under GDPR is illegal and cannot be consented nor under GDPR nor under e-privacy. But what we did knowing that these digital worlds are a little bit different to our old analog world is that the proposal broadens the possibilities to process metadata and also consent data. But it is very often difficult to decide if it's really a good idea to process metadata or even content date. And that's why we said, if you want to use these broadened possibilities for processing data, in that area where we allow it, you need to ask for consent.

So it may be that I agree. It's a good idea that you follow me through the town because I think if you use that data to find out if we can improve, I don't know, the walking ways because I'm very often walking. But in that town, there are only streets of cars, no ways for walkways so you could check with that or any other thing. Maybe I like to be profiled because you give me good advice which dresses I should buy next year because they are very in and whatever. If you like to do so, you can consent.

So many things stay illegal, many things might be used from your personal data but then you have to ask for consent. And then coming back what you already pointed out, that consent needs to be very specific. So you have to explain to the individual user, what are you doing, why are you doing it, what will you do with the data, what is the purpose and then the user is to say, okay with that information, I agree that for that purpose you can use that data.

MR. KERRY: So let me ask a follow up to that question. Because in some sense, it brings me back to where we started the discussion. Why this on top of the GDPR? If tracking, if consent is required for tracking and tracking is already illegal under the regulation and under the directive, why this legislation? You've described it as an expression of, you hope to abolish surveillance driven advertising. If that is what this is about, why is it necessary on top of GDPR if it is already illegal?

MS. SIPPEL: It is already illegal under the e-privacy directive. Secondly, so far that's the European Union thing how to do legislation. With a directive, you create a minimum level of rules but every single member state can add something. You can't lower the level that you give but you can add something, you can improve, you can offer your citizens a higher level. So, so far we have had directives so very different levels of protection. That's one reason why now we are doing regulation because a regulation is a regulation and you have to use it like it is in all the 28 member states. That's one reason.

The second reason is that, as I said at the beginning, not all forms of communication were protected. Because we made the mistake to talk about precise things like emails, SMS but technologies have evolved. So we forgot about other services and that's another reason why we have to work on e-privacy to create one rule. The other reason when talking about tracking, maybe at the very beginning we thought the old fashioned idea, my newspaper will follow me and it is only my newspaper looking into my data but now we know it's something else. The whole world maybe will follow me because my data is sold all the information to the whole world. And that is something where we say, that's not possible and it was not in the

proposal from the commission in e-privacy.

But clearly the Parliament says, okay if there is a service offered, you can't have this tracking wall. So you agree that all your data are collected and sold to whoever is ready to pay so we want to have a ban on the tracking wall. The reason is that we say the access to a service and the analog it will be going into a shock, going to a ticket shop to buy a ticket for the train or for a museum something like that. Going to that area and using that service couldn't mean that you exempt surveillance measures. If I go into a shop or ticket counter, it is not necessary that first I tell them, oh my name is Brigit Sippel, I'm living in Germany. Last time I visited the following ten web pages. I like flowers. In my garden I do have tomatoes and blah, blah, blah. I don't need to give that information simply to enter a shop or enter a ticket counter to buy a ticket. But in the internet that is happening right now and we want to stop that.

MR. KERRY: Yes in the back on the left.

MS. BASU: Good morning, I'm from India. My name is Dia Basu, I'm a PhD candidate at American University here. My question is to find out how much collaboration there is between EU at bilateral or multilateral forums in informing data protection, regulations of other countries. I'm particularly interested in India because it is currently in the process of framing its own data protection regulations. Thank you.

MR. KERRY: We'll take the other question.

MR. COCHETTI: My name is Roger Cochetti. I work with private equity in the technology sector. My question is due to the broader aspect of all of

this, you haven't discussed too much and that is surveillance and enforcement mechanisms. As, I think, anybody who has dealt with this subject knows, a great deal of this is going to come down to the specifics of enforcement. Using the metaphor a few minutes ago, if someone were to ask, may I touch you, and I say sure, and then you punch me, did I give consent. That's a form of touching. If I asked the question in Flemish and you respond in Greek, have I given you specific consent to touching when you're punching.

So enforcement is going to be 99 percent of this and could you discuss a little bit of how you will actually surveil the agreements that are incurred between service providers and individuals. And how you would then enforce them, enforce your regulation once you've surveilled the text or the terms of these agreements in multiple languages. Thank you.

MS. SIPPEL: The first question on how do we connect with others to inform them having in mind that those rules shall apply to everybody offering services to people in the EU. Now the first thing is that within Europe, we all informing all the member states, of course, because they are involved in the process. Then we have a lot of international contacts, why are our different parties in Parliament. The commission has their own contact to inform everybody about the new rules. I think there is a networking inside Brussels, for example, between the commission and the different embassy's that are there on an international level. Also, many NGO's are very active, data protection activists and we have a European data protection officer. We have all the other European data protection offices. They are linked to partners all over the world.

I think India is a very good example for the time being about the good effects of GDPR. Because we were just informed that some time ago, India decided that yes, data protection privacy is a fundamental right and you are starting that. So I hope you and other people from India who are able to take part this week in the IAPP conference to get more knowledge. Of course, you also should follow the detailed information from the commission. Because we not only create the law but the commission on all our data protection offices are giving additional advice on how to deal with the different parts and if you contact them, that's fine.

The question how to follow and ensure that the rules are implemented to that clear question on touching or doing something else. Now first of all, that's why asking for consent you have to be very precise, that's one thing. In general terms, we strengthened the role of data protection officers also demanding impact assessments whenever you are doing it and we are strengthening our national supervisory authorities so that they can control if all the actors are ready to do it.

In addition, you are completely right. If you ask in Dutch and you answer in Greek, there might be a problem and how do you control it. So first of all, you need to ensure that your user does understand what you say. So if you are coming from Greece, you offer a service to Germany. Of course, you should offer that Germany also in German language otherwise no one would use your service, that's the one thing.

Then the question of control. Did I really consent to what you did in your example. So in whatever form you ensure, the moment I give consent, you as the service provider, the service you have to ensure that you always can prove I

gave consent. If I do it by writing a letter, yes now I do consent to that or if I do it via an email or you organize it in a way that is a technical question that I put it in the internet page. But the question and my answer will be electronically stored so that you can prove on the 1st of January here I can show you, you gave consent. But every company needs to find their ways, they can ask for consent but then they have to prove if, when and what for purpose I really gave consent. So if there is a conflict, there is also proof for that.

MR. KERRY: So one question to wrap it up because we're coming to the end of our time. Yesterday at the Privacy Professionals Conference, you described yourself as a chief negotiator for the Parliament with nothing to negotiate because the European Council hasn't formulated a position yet. Looking ahead, what do you expect from the Council both in terms of timing and in terms of substance. Will this be done before the mandate of the Parliament runs out next year?

MS. SIPPEL: First of all, saying I have nothing to negotiate, that's the official situation. Because officially, negotiations between commission Parliament and Council as a representative of our member states, can only start after the Parliament has done its job, the member states also have a position. But, of course, unofficially, I do try to get information from different member states from the Council on how far they have done things but that is under the radar. It's informal meetings that we are doing.

Official meetings now member states announced that maybe they have a position on the 8th of June. So let's see. For me, it's a little bit late because

originally the idea was that GDPR and e-privacy should apply at the very same time. But okay, member states need some more time. So now 8th of June is in their calendar. I wouldn't be sure it will be date but in case it is, then after the 8th of June we can start the official negotiations. If you now would like to ask me how long that negotiations might take before we have an agreement, that clearly depends on the very precise position that the Council is coming up with.

MR. KERRY: In terms of position, what do you expect the issues to be?

MS. SIPPEL: So I will not be very precise but it is without any question that the position of the Council will differ from the position of the Parliament. But I hope with some good will from the Council and from our side, of course, we could have a decision at least this year.

And I also hope that after the allegations regarding Facebook and Cambridge Analytica within the Council, there is now more awareness that data protection and protecting privacy is not only something, on it's nice to have it, but it is really something important. That hopefully will affect their position on e-privacy in a positive way.

MR. KERRY: Well thank you very much. I'm sure more people will be watching the process as you move forward.

MR. SIPPEL: Thank you.

* * * * *

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