Third Annual Detlev F. Vagts Roundtable on Transnational Law: Data Protection in a Global World

Low, L.; Vagts, K.; Schwartz, P.; Irion, K.; Stevenson, H.; Brunner, L.; Wimmer, K.

DOI
10.1017/amp.2019.123

Publication date
2018

Document Version
Final published version

Published in
Proceedings of the Annual Meeting - American Society of International Law

THIRD ANNUAL DETLEV F. VAGTS ROUNDTABLE ON TRANSNATIONAL LAW: DATA PROTECTION IN A GLOBAL WORLD

This roundtable was convened at 11:00 a.m., Friday, April 6, 2018, with opening remarks by Lucinda Low, president of the American Society of International Law. After additional welcoming remarks by Karen Vagts, Paul Schwartz of the University of California introduced the participants: Kristina Irion of the University of Amsterdam Institute for Information Law; Hugh Stevenson of the Federal Trade Commission Office of International Affairs; Lisl Brunner of AT&T Services, Inc. Global Public Policy; and Kurt Wimmer of Covington & Burling LLP.

Introductory Remarks By Lucinda Low*

doi:10.1017/amp.2019.120

Let me welcome all of you, on behalf of the Society. I am Lucinda Low, the president of the Society, and we are delighted to be here at the Third Annual Detlev F. Vagts Roundtable on Transnational Law. We have a fascinating topic that our panel today is going to explore, but first I want to say a few words. We are so delighted that the Vagts family came to us after Detlev's death to carry on his work and thinking in the area of transnational law. He was a pioneer in so many ways, and did so much to develop the contours of the area of transnational law. We are very grateful to the family for their generous gift, which has enabled the Society to create this annual event.

This is a very special year of the Vagts Roundtable because we have not just one but both of Det's daughters, Karen and Lydia Vagts, here with us today. Would you please both stand up and be recognized.

Remarks by Karen Vagts

doi:10.1017/amp.2019.121

Thank you all for coming. Dad was the only lawyer in our small, tight-knit family, and we really did not know what he was about because at home he was very modest, but we knew every spring he was headed to wherever the ASIL conference was. After he passed, there were so many wonderful statements about him, and we realized what he was doing was important and what he was working on we would like to find some way to continue. We were eventually pointed to ASIL by particularly Peter Trooboff and Harold Koh, who will be conversing later today, and it made sense because this really was Dad's community.

We tried to think of what might be appropriate and we figured out, with the assistance of the ASIL leadership, that it should be something about transnational law, business, and ethics. We also wanted it to have some practical aspect because even though Dad was an academic, he was very much shaped by his various work experiences. The idea of the roundtable came up, and while it focuses on the intersection of those three issues, the topic varies from year to year.

This year it is data, and did you know what was coming with some of the issues that have been in the news when you planned this, because it is very timely. What is interesting, when I think of what

* President of the American Society of International Law.

Dad might have thought about it, if you mine the data in the Google Ngram database, which scours Google books for words on a longitudinal basis, while collecting data is an ancient activity, the word was not really in common use until starting in the '50s and '60s, when Dad started his practice. He would not have discussed any of these types of issues using data, probably. I am not sure what he would think about it but he would know that it is very important to get a grip on this fascinating topic, which undoubtedly is going to be impacting all of your work in the years to come. We are looking forward to hearing what the roundtable discussion says.

Lucinda Low

Thank you very much, Karen, and let me just reinforce that a number of ASIL leaders, including, as Karen mentioned, Peter Trooboff and Harold Koh, as well as Hannah Buxbaum and Lori Damrosch, who have had a role in the roundtable, and Hannah, in fact, served as the 2017 convener and assisted in the planning of this year's program.

I would also like to thank our convener for this year, Joel Reidenberg, of Fordham University School of Law, who did an excellent job of organizing the program but is not able to be with us in person today. But we have, as our moderator, Paul Schwartz and let me now introduce him. Paul is the Jefferson E. Peyser Professor of Law and Co-Director of the Center for Law and Technology at the University of California, Berkeley Boalt Hall School of Law. We are very grateful to him for taking on this important role, and it is now my pleasure to turn the proceedings over to him, to talk about data protection and the word "data" in a global world. Thank you.

Remarks by Paul Schwartz*

doi:10.1017/amp.2019.122

Thank you so much, and I would also like to thank Lydia and Karen, and tell you that Kurt Wimmer told me that when he told his partners at Covington that he was going to speak here, just how many of them remembered Professor Vagts with such fondness, and just how the ripple effect of his life has been felt by so many. Thank you for being here and we are all very happy to remember Professor Vagts' memory, and to cherish it with you.

Now it is my great pleasure to introduce Kristina Irion, assistant professor at the University of Amsterdam Institute for Information Law, who will be presenting her paper on situating privacy and data protection within trade laws, such an important topic.

Remarks by Kristina Irion†

doi:10.1017/amp.2019.123

Hello to everyone. It is sometimes difficult to come from Europe and talk about a rather formalistic legal approach to data protection to a legal audience in the United States. I have to say when I read the *Wall Street Journal* at breakfast, it was a good moment. They are not going to rip me apart.

I am very happy and I am very thankful for the invitation to this Vagts Roundtable today. I am joining you from the University of Amsterdam, from the Institute for Information Law. For twenty-five years we have been doing—not me, personally, but many of us—research into the normative framework of information law that stretches various domains, and yes, this topic is getting increasingly important. I am specialized in privacy and data protection now, at the crossroads of international trade law.

* University of California.

† University of Amsterdam Institute for Information Law.

I would also like to thank the convener, Joel Reidenberg, who cannot be with us here today, for assembling this really wonderful roundtable, and Professor Schwartz for the nice introduction. I also believe that Professor Vagts would have very much liked this topic, that really takes all the things you said earlier about transnational law, economic relationships, and ethics in context.

After a brief introduction to the topic to set the scene, I will present the main gist of a co-authored paper on the interface between privacy and trade law. And I would like to just start with some thoughts of Professor Reidenberg, because he believes that states must be able to afford protection to their citizens online. He also prognosed already, back in 1999, that inevitably trade law will become involved in privacy issues because data flows and personal data are intertwined.

As we speak right now, a trade war looms between the United States and China, which has the potential to harm the rule-based multilateral trade system, but it is about trade in goods. Digital trade and services, by contrast, behave somewhat differently, and it must be considered, of course, that data flows substantially underpin digital trade. Many popular online services, many of them from the United States, would not otherwise be delivered to users on a global scale.

In recent international trade diplomacy, parties negotiate new commitments with respect to data flows. New data flow language has entered the transpacific trade partnership, the TPP, from which the U.S. government pulled out last year. It was also on the table during the negotiations for the U.S./EU Transatlantic Trade and Investment Partnership, the T-TIP, and the multilateral Trade in Services Agreement, the TiSA. All of these negotiations are stalled right now over uncertainties regarding the new administration's trade strategy. However, the U.S. Trade Representative, Mr. Lighthizer, already resurrected the data flow negotiation objective in the NAFTA negotiations.

Outside of the United States we also deal with data flow requests. For example, the EU has just negotiated a trade agreement with Japan, the JEFTA, and Japan really very much wanted to see a clone of the language that they already agreed to in the TPP also being put inside the JEFTA agreement, but that did not take place until now.

Next to state actors there are numerous initiatives of trade institutions and think tanks that laboriously argue the point of data flows as well. I would like to recall the World Economic Forum. There is a new think tank that is built at the WTO with the participation of the World Economic Forum and funded by Alibaba, a Chinese large internet retail company that also wants to improve the digital trade agenda, as it is called.

Now data flow, I am convinced, also needs human and societal values engrained into its fabric, and this is a true challenge for international economic law and any rule-based intervention. This is not just about online privacy but other issues in other contexts too. Today it is Microsoft's Brad Smith calling on governments to adopt a digital Geneva Convention to protect civilians on the internet. He is worried about states and that they should abstain from cyber-attacks, for example, that target the private sector or critical infrastructure.

Online security is just another facet of values in data flows, together with consumer fraud, unfair trade practices, surveillance, and, of course, user privacy online. In practice, governing data flows turns out to be a rather difficult enterprise. There are two reasons for that. One is, of course, as we know, and as you have also very nicely described in your recent paper, Professor Schwartz, there are stark differences in local standards of protection. Just take information privacy, for example. Second, principle, it is very, very difficult to govern anything that is essentially volatile, and this has always challenged traditional public policy.

Now let me turn to the European Union. Its comprehensive data protection law has always been controversially discussed, here in the United States as well, and the European legal tradition and instruments are, of course, necessarily very different from U.S. law. Nevertheless, now there are online privacy scandals on the front pages of U.S. media, and I read some very forthcoming accounts yesterday about the new General Data Protection Regulation in Europe. I hope this

will make it easier to generate acceptance for the rationale to defend a high level of personal data protection, and that is what the European Union is actually trying to achieve now also within its trade mandate.

Just a little background for you to situate why EU-style data protection law may be too big to fit inside the established trade law system. You are probably well aware that in our constitutional law the right to the protection of personal data is protected as a fundamental right next to the traditional right to privacy. In contrast to the United States, in Europe such rights are vested to everybody, to EU citizens, to residents without citizenship, and even tourists. If you travel through the EU you can rely on that.

Next, you have judgments of the EU's highest court finding in favor of a right to be forgotten, and of course, the one invalidating the safe harbor agreement with the United States. You are well aware that by now the privacy shield governs personal data flows from the EU to the United States, but that many firms also rely on different legal mechanisms to export data. Of course, very important at this moment: the countdown to the General Data Protection Regulation, which we call GDPR, is almost up. On the 25th of May—this is pretty soon, this year—the GDPR will enter into force and this will bring a few regulatory innovations. Innovation happens also in lawmaking, of course.

I will give you some flavor of it. For example, there will be the right to data portability. That means users can take their data that they have uploaded from one provider to another provider, and ideally this will be ported directly between the providers. But also, there will be mandatory privacy impact assessments for certain situations, data breach notifications, and so on.

Within the GDPR there are two mechanisms that specifically aim to regulate data flows. The first one we know already. When Europe exports personal data, it actually also wants to export its regulatory approach. This is the reason for the privacy shield, which is, in a way, an international agreement in which a number of the provisions that we have in EU law are then also a commitment for U.S. receivers of EU personal data. But also, other safeguards exist that are used to establish obligations similar to what we have, and that travels with the data. In a sense, personal data is supposed to travel with regulation attached to it.

The other mechanism is new. It is very new, and it is an experiment with a very uncertain outcome. The GDPR turns around the logic of the territorial scope of application. Instead of attaching the law to where the provider is established—so necessarily this has to be done within the territories of the EU—now the law applies to where the user resides. Whenever there is a business collecting data from data subjects that are inside the EU, and they are selling a service or a good, or they are starting to monitor online behavior, then they would need to apply the GDPR as a whole. That is a huge regulatory export, I realize that too. And this may sound outrageous from outside of the EU. I understand that as well. But it is a response to practices that essentially deprive 500 million EU citizens from domestic data protection standards.

We have seen, until now, in the courts and with administrative procedures in the European Union, that companies and businesses frequently raise that there is no sufficient nexus for jurisdiction and that the applicability of local laws interdicting certain behaviors does not concern these businesses. These arguments have been used in order to basically deny the authority of EU regulations.

One less-known aspect of the right to be forgotten ruling is that the Court of Justice in the EU has adopted a much more holistic view in which it connects the revenue-making activities of an organization with its free online services. The justices find in favor of the application of EU data protection law if there is a free online service and there is, at the same time, a revenue-making activity like selling advertisement to local businesses or to local companies within the EU. It is akin to the follow-the-money approach. And that was also, in that moment, dismissing the argument of Google in this Google Spain case, that there is no jurisdiction. What the GDPR is doing is taking

the jurisprudence from the highest instance in EU law and putting it into practice now with the new regulation's scope of application. These changes are certainly also a reaction to the many failed attempts to get some meaningful self-regulation off the ground, just to recall the failed industry standard on the do-not-track browser settings, which could have empowered users against a pervasive tracking and monitoring online.

This is the GDPR, which you may criticize for being overly formalistic and complicated, but it is the legal instrument the EU is bound by also when making new trade rules with other countries. Against this backdrop, our paper discusses the intersection with international trade law and EU data protection rules in relation to data flows. This contribution breaks through a very common compartmentalization between different scholarships. Even though we are all lawyers, there are privacy lawyers and there are trade lawyers, and they often do not speak the same language. It is sometimes important to actually bring the two together, and to our impression, this even has divided EU institutions. The EU is not a monolith. It is a giant bureaucracy and also in there both camps did not talk to each other. They did not know of each other but their field of competences was actually growing together more and more, and they should talk to each other.

Our main objective has been to analyze how far the two legal regimes would clash and to offer recommendations that are addressed to the EU policymaker regarding how they can avoid inconsistencies between the two policy areas. Our argument basically follows three different parts. The first one critically engages with the narrative of data flows being free of human and societal values. In the second part, we trace how data flows entered trade diplomacy in the past and have gradually been endorsed in some international trade deals that have been concluded, and it is definitely very high up on the agenda whenever new trade discussions take place. And our last part is about the EU perspective and the process that has let within the EU institutions to negotiate a position between trade and privacy that joins them up, and with which they can go into negotiations.

On data flows, this contribution underscores that there is a positive feedback loop between the flow and digital trade. That is very intuitive. There is nothing wrong with that. But we very critically engage with the empirical data and the methodologies that frame this discourse today. International organizations, both intergovernmental and also influential think tanks with a trade mandate, cite exactly these numbers. Everyone cites these numbers.

The McKinsey Global Institute that is a think tank within a consultancy estimates that global data flows raised the world GDP by $2.8 trillion in 2014. That is a massive number. It is very impressive, obviously. And against the background of this overwhelming number it is argued that the EU approach to personal data protection is overly restrictive, onerous, and protectionist. That is basically the gist of this logic. We are trying to work with the numbers as far as a lawyer can work with numbers. I mean, we have limitations. But we try to engage with this argument and with the methodologies, and actually this much-cited McKinsey report has a section on their methodology where they list a range of limitations and problems and uncertainties with these kinds of estimations. But this, of course, does not come when everybody recycles and uses this number. This number stands there and there is nobody anymore looking at this huge luggage, how this number was derived and how approximate it is.

There is, at the moment, no reliable measurement of data flows, and assessments of data flow's contribution to value creation lack solid methodological grounds. There is, at the moment, no good methodology to assess, for example, how much value was generated by trade in services, and, of course, many services have been already delivered electronically or via networks. What we see in this number is some sort of double-counting. There is a certain number that is already realized when you make statistics about trade and services, and then, in addition, there is now this value from the flow, but actually this is already within the trade in services, just to give you an example.

The next criticism we have is that the whole extrapolation from the estimation of data flows and their value to the effect of domestic privacy regulation results, in our opinion, in a screwed picture.

Basically, you cannot take this number, this big number, and say that is why your data protection law is onerous. If this number is true then this has been realized with EU data protection law, actually. What is the onerous part?

There is, of course, a regulatory burden. Every regulation places a regulatory burden on enterprises. And yes, there have been surveys being conducted here in the United States and for U.S. businesses that are having business with the EU, the GDPR or its predecessor is a burden, obviously. By the same token, say, Swedish companies that were asked whether this is a burden, find this burdensome. But many normative regulations are creating a burden, and we want that. We want traffic safety, for example. We want many other standards to be realized that are a burden, but they are good for us.

And, thirdly, framing the protection of personal data as a barrier to trade ignores broader societal values and normative rationales for affording a high level of data privacy protection. We could actually say that data flow is good just because there is protection inside. Then it is good. If it is just a flow—and that brings me back to the earlier argument on cybersecurity and many other issues—flow is only positive if it is a good flow, if it is a safe flow, if it guarantees certain values. And, of course, we have to recognize that the world has different standards.

Essentially, we conclude that the data flow logic is overplayed in the trade diplomacy in a way that legal scholarship researches as an imaginary. It is a framing. It is a narrative, and within this narrative it creates a very important motivation for governments to endorse the flow and maybe forget a little bit about the values. We can also turn it around and basically talk about the values and make the flow part of the value discussion. That is what we call an imaginary. There is a lot of scholarship on that but it is not, in practice, very relevant, I guess.

We get now to the digital trade agenda. The recent discourse on the importance of data flows for digital trade is not an entirely new issue but arises from previous work in the WTO on electronic commerce that was later then relabeled as digital trade. It sounds better. The U.S. trade negotiators have been very successful in setting and defusing the digital trade agenda in bilateral trade agreements, for example, with South Korea, and the TPP.

Data flows, however, are also not entirely new to WTO law and there are two predecessors of data flow clauses in service sections, on financial services and telecommunications, which are annexed to the GATS, the general Agreement on Trade in Services. Both commitments are, in themselves, subject to counterbalancing provisions on privacy and confidentiality, respectively. So, there is this guarantee of the flow in telecommunications or financial services, together with counterbalancing provision that tries to say but if you put this regulation in place and ensure confidentiality of communications or financial secrecy, this is just fine. That is also tolerated.

If, however, a country's domestic regulation violates trade law this regulation has to be justified as part of the general exceptions. In trade law, the general exceptions are a construction that creates a certain margin for parties to a trade law agreement to have a certain autonomy to regulate, to make domestic regulations. And legal scholars have already suspected that some features of EU data protection law can violate the GATS disciplines and they may not be capable of being justified. Even without this new flawed language in trade law we have, right now, likely a problem with the GATS.

If we take, for example, the adequacy findings by the European Union: A number of countries have good reason to be jealous of the United States and suspect preferential treatment, because the United States gets, rather quickly, a new arrangement to exchange data with the EU, which is, of course, also a token for the important trade relationship between the EU and the United States, but other countries are queuing for years, and this is not always fair.

There may be other issues, such as whether the new right to data portability is really necessary to protect privacy or if implementation measures arbitrarily discriminate between countries.

It also—and that is a big, big "also" here—it is also really unclear whether a party to a trade agreement can take measures against another party's state surveillance laws without being sanctioned under the trade law.

The upshot is that without internationally accepted standards of privacy and data protection and also surveillance, the GDPR is too big to fit inside the margin that is left for regulatory autonomy of a party to any trade agreement. And that is why the EU had a problem, and this problem came at an inconvenient moment because the EU was just in the heat of the negotiations of T-TIP and the TiSA, as I mentioned earlier, and they did not have a position that was actually backed by all EU institutions—the European Parliament, the European Commission, which is our executive, and member states, obviously.

In this last part I focus exclusively on EU policy. It is a bit alien when you are not from the EU, because it has its own nomenclature and works very different. But I tried to keep it understandable.

The EU has exclusive competences for two policy areas—to negotiate international trade agreements, that is external trade, but also to make law on data protection and also to govern transfers of data to other countries outside of the EU. That makes the EU, in this field, extremely powerful, because in these two fields, member states cannot make their own policies. It all will be channeled through the EU. And this is what we often call, in international law, the Brussels effect. Through the Brussels effect regulations are getting much more powerful when they are uploaded to the EU level instead of when member states run around, in separate instances, trying to do something. This Brussels effect you will also see, maybe if Facebook would indeed adapt the GDPR, as Mark Zuckerberg yesterday said, for the entire world. We will see that.

So, in a way, what should happen is that if the EU has these competences for both these fields then you would think they have a joined-up strategy, basically, that aligns their privacy strength with their external trade policymaking. This has only partially been true. The Commission, that is the executive of the EU, promised that it will seek to use free trade agreements "to set rules for e-commerce and cross-border data flows and tackle new forms of digital protectionism, in full compliance with and without prejudice to the EU's data protection and data privacy rules." That is from an important strategy of the Commission.

However, in its negotiation, the EU trade negotiators actually relied on the robustness of the existing exception in the GATS Article XIV, to preserve the EU's autonomy to regulate privacy and personal data protection. So, interestingly, it was the European Parliament which underscored the need for better scoped exceptions in free trade agreements. After all, the European Union is not a monolith in itself—I said that earlier—and it took a year of backdoor negotiations between the various decisionmakers at the EU, including the different units of the European Commission, to finally arrive at a compromise text. This text, which is endorsed by six commissioners, including the commissioner responsible for trade of the EU, Cecelia Maelström, resolves in favor of an unconditional counterbalancing clause on domestic privacy and data protection regulation.

So, to conclude, in fact, it was a good moment in time that the negotiations on TiSA and T-TIP stopped for a moment, because I am sure this will resume at some point. This is not going to be forever, like this. But it gave the EU, which is also a complicated, multilateral organization, the time to actually hammer out a sound approach, and an approach that tries to have both data flows but with data protection. And maybe this is for the benefit, if that becomes a standard, inside trade law too.

I am happy to say that our institute really assisted in this effort, because we have been consulting the EU on this whole trade and data protection intersection, and this is going to stay with us for the future. This is a very important topic. How we want data flows and how much they should carry values is something that has to be determined now. What the EU says in the negotiation with other countries is also not automatically becoming then a rule. Obviously, there is a negotiation going on,

but it is a very good start to have a position that does not threaten its own EU data protection standards, that ensures the consistency of EU law, basically, before you enter a negotiation.

While I am not saying that EU data protection law is in every aspect a gold standard for how to do things with privacy online—and I have criticism here and there about this or that—it is at least a standard. Having a standard is sometimes better than having none. And I am convinced that we should not institute data flows without effectively protecting privacy online, also within the trade diplomacy.

And with that I leave you. Thank you for your attention, and I am very much looking forward to the panelists' comments. Thank you very much.

Paul Schwartz

Thank you, Kristina. We are now going to introduce our respondents. We will hear next from Hugh Stevenson, who is at the Office of International Affairs at the FTC, and then from Lisl Brunner, who is at AT&T and doing global privacy there. And then after that we will hear from Kurt Wimmer, who heads the data privacy and cybersecurity practice at Covington & Burling here in D.C. So, Hugh, share your thoughts with us.

Remarks by Hugh Stevenson*

doi:10.1017/amp.2019.124

When I checked in I asked, "Well, where is this session taking place?" and they said, "In the Hall of Battles," which I thought sounded a little ominous, because there are some tensions involved in this topic of privacy, and particularly privacy and the free flow of information.

I very much appreciate being part of this discussion, and it is really fascinating to hear all of the issues that have been raised. It is a real challenge to respond. The paper here covers such a sweeping scope of issues with such erudition, and it is challenging to get into a lot of it, but I would like to focus on a couple of things.

I do have to provide the disclaimer that my views are my own, not necessarily those of the Federal Trade Commission. And I also want to disclaim that I am not a trade lawyer, despite working for the Federal Trade Commission. For those of you unfamiliar with the distinction, there is the U.S. Trade Representative that leads the U.S. trade efforts, and Kristina referred to them.

Our role is really more focused on consumer protection and privacy as part of that function. And we have an enforcement function. We bring cases. We have brought over, I think, five hundred cases of various sorts involving privacy issues. We have a summary online—I will not go on more about that—of the kinds of things that we have been involved in. We also have done a number of reports and conferences on all sorts of privacy cutting-edge issues.

I am from the international office, and we follow with great interest the developments in the EU, both on the policy and enforcement sides. We work with a number of the DPAs, well, around the world, but including in the EU. We have memoranda of understanding with three of them, I think, on data protection issues—UK, Ireland, and the Netherlands. We have been involved in the Safe Harbor for many years and the Privacy Shield negotiations and implementation, and followed the GDPR with interest.

There is so much here, both to, I think, agree with and to disagree with. It is a very large area and there are a number of different kinds of issues, and some of the criticisms actually I think Kristina had touched on. There are some commonalities too. I mean, if you look at the GDPR, which was the product of extensive legislative discussion, you see some things that are really very familiar—

* Deputy Director, Trade Commission Office of International Affairs.

in fact, maybe in some cases, inspired by United States developments. The data breach notifications, for example, referred to the Brussels Effect. There is also the California Effect, and California had the data breach law, and now I see Alabama has checked in as number fifty of the states that have enacted such laws. That is one example of an export of that idea. The accountability work that has been done in the United States is another example. There are other areas, on the other hand, where there are more substantial differences. Maybe the right to be forgotten issues that you mentioned, or data portability; perhaps, some other areas.

One of the interesting things about this paper is focused on the issue in particular of data transfers, and in general European law, it is fair to say, has had a focus on geographical destinations of data. That has been an issue. Indeed, I am not sure it is a new paradigm. In fact, I think it is the old paradigm that we have had some tension between data transfers and privacy. I was looking back last night at the Council of Europe convention and the provisions there. And, in fact, there was one scholar who said, the convention contains this article stating that "despite the need to protect privacy, a free transborder flow of data should not be obstructed." That was not a USTR representative. That was Spiros Simitis, one of the leading names in European data protection.

Similarly, in the OECD guidlines in the 1980 version, you see that language both about the protection of privacy but also the free flow of data. Similarly, in the 2004 APEC privacy framework you see an acknowledgement of the need both to protect privacy and the free flow of data.

One interesting aspect of the paper that Kristina touched on here is thinking about how you measure those benefits, which I think is a really interesting subject, although, at the same time, it is something that has been part of the calculus going along. Exactly how one thinks about that is an interesting issue, and how one evaluates those numbers. It did prompt me to think about some numbers that we have seen in connection with Safe Harbor and Privacy Shield. Some of the data transfers involved the large sort of operations that are a focus of great interest and in the news and so forth. But there are also a lot of the data transfers that involve HR data, which is not necessarily a cutting-edge issue so much as a necessary part of certain multinational operations in transferring data. And similarly, the number of small-to-medium enterprises that have been involved in those transfers is a substantial one. One thing about the Safe Harbor and Privacy Shield systems is you can see exactly who is on it, who is using it, what the companies are, in a way that you cannot see in one of the other major measures used, the model contracts provisions.

The focus on data transfers is interesting also because there are two mechanisms that are particularly noteworthy here. I think that Kristina mentioned both. One is the extraterritorial application. The '95 directive really did not focus so much on the extraterritorial reach as a strategy, let us say. The new law does. And that is something that, in some ways, is familiar to us in certain U.S. contexts, to antitrust law in certain extraterritorial reaches. When we amended the FTC Act to deal with consumer and privacy issues, in fact, one of the things we did was we wanted to clarify that we had extraterritorial jurisdiction to protect organizations operating outside the United States, if they were victimizing Americans. And similarly, the other way around, if there was substantial conduct in the United States targeting others.

The other strategy, though, I think is less familiar to us, and that is the "adequacy" determination that was mentioned, and I think this is an area that may be a good example of the application of the criticism Kristina mentioned about being overly formalistic—well, she used a number of adjectives that I will not repeat, but I liked hearing them. One of the things worth looking at about that sort of frame is that this is the system of determining the adequacy at large of a country, and this, I think, has been subject to some criticism. The former Canadian Privacy Commissioner wrote an article recently, for example, looking at this, and had a number of critiques of them. One, the sort of extraneous issues that might affect who was in line to get the evaluation.

She did a chart correlating when a country hosted the International Conference of Data Protection and Privacy Commissioners compared to when they got adequacy.

Similarly, one might not think that the Faroe Islands and Andorra would be at the top of the list for these kinds of evaluations, and other scholars have pointed out that, for example, Argentina got adequacy before they had brought any enforcement action or, in fact, implemented their law. She points out a number of other issues, including the indeterminacy of the calculations. At the time, the Quebec Privacy Commissioner asked, for example, why the EU authorities involved at that time took initiatives to help Monaco adjust its system but did not do the same for Quebec.

And this is a system, in a larger sense, that I think one would ask, it has been around in the form of the '95 directive since '98, and written in '95, and yet we still have a really small percentage of the world population that really has had even the question of adequacy addressed. Part of the paper here is talking about, if there is a conflict between trade law and these privacy issues is that a problem with the trade law? I cannot answer that, in terms of the trade law analysis, really. I mean, I followed it.

But the other question is, is this really that bad a result to say that this part of the approach here, which has been criticized by various scholars, is that really the thing that needs to survive? And one thing that was interesting to me is that this was the main example that is often given, and I am not sure, though, that it is really the item that is most fundamental about the fundamental rights that we are talking about.

The last point I want to make is, to think about that: what is fundamental here about this fundamental right? I do not ask that rhetorically but rather [showing a copy of the legislation]—this is a copy of the GDPR. It is a big thing. Is it all fundamental? I mean, there are certain provisions that are fundamental. There are, I think, about four sentences in the EU Charter, a sentence in the European Convention on Human Rights, and there are clearly key issues. But is all the implementation fundamental? Is the implementation of the registration of databases fundamental? Apparently not, because it used to be in the law and now it is not. Is it important to areas at the margin, because the '95 directive gave some margins of maneuver for various states? Some required things that others did not. Were those fundamental? Well, apparently not because they were not required of every state.

I think one issue to think about here is what is it that, in substance—and maybe this is not so much the trade lawyer's point but the privacy lawyer's point—is really fundamental here to protect, and is it a mechanism, for example, like "adequacy," or are there the other values that really are the ones that are keyed on and might properly be the focus?

I will stop there. I do have to acknowledge this paper—I see it was not written for me. It is about what the EU negotiation position should be in connection with the Americans, of which I am one. But I think it is a very interesting topic, and I appreciate it being pursued.

Thank you.

Paul Schwartz

Thank you. What I have proposed is we will hear from Lisl and then Kurt and then we will give Kristina a chance to respond.

Remarks by Lisl Brunner*

doi:10.1017/amp.2019.125

Great. Well thank you to ASIL for inviting me, thank you to Joel and Paul for inviting me, and thanks for the chance to read the paper, which I really enjoyed. I thought it was really thought-

* AT&T Services Inc., Global Public Policy.

provoking and it made me want to go through and read all the citations that were cited in the footnotes, which is always a good sign.

I will give you a policy perspective, because I am also not a trade lawyer, and perhaps some of these impressions are very consistent with what a multinational company like AT&T supports, and some of them are my own. But reading the paper I also tend to agree that there need not be a dichotomy between the protection of privacy as a fundamental right and the promotion of cross-border data flows. Legal regimes can protect both of these values simultaneously, and I think there is a very good argument to be made that the EU legal regime does that.

A legal regime that restricts the cross-border transfer of personal data in order to protect its subjects' rights should do so in a way that is flexible and predictable, in order for it not to look like a restriction of trade and services. And there is also a need for greater interoperability among the legal regimes that limit cross-border data flows.

EU data protection law is flexible and it arguably strikes an appropriate balance between the fundamental right of individuals to the protection of their data and to the member states' interest in furthering international commerce and the free flow of data. The GDPR and its predecessor provide for multiple bases for transferring data, even though they seek to restrict it. There is the adequacy basis, which also has given rise to Privacy Shield, so there is a little bit of flexibility in adequacy. There are appropriate safeguards such as the model clauses, binding corporate rules that companies can adopt. And then there are several bases for ad hoc transfer, either one-time transfers or perhaps a limited number of transfers.

That is fairly flexible. It is the less-flexible regimes that I would think present more problems for the free flow of data and for trade agreements. Argentina basically only allows adequacy and consent, and a few other very specific exceptions for the transfer of data, and Brazil, when they were debating a new data protection regime, adopted something very similar, which has not yet passed into law. In South Korea, consent is the primary basis for transfer, meaning that the data subject must consent to each transfer or to the regular transfer of data across borders. That is not particularly flexible. South Korea is looking at joining the APEC cross-border privacy rule system, which I will mention in just a moment, so that certainly helps on that front.

The restrictions to the free flow of data also have to be predictable. In 2015, in the *Schrems* decision, the Court of Justice of the European Union declared invalid the European Commission decision that the United States had an adequate legal regime, based on the Safe Harbor Agreement. This had the potential to suspend a large volume of cross-border data flows.

The Court was never asked to do this. Max Schrems did not ask the Court of Justice to declare the agreement invalid. And it also did so without having in the record a study of what U.S. law on surveillance was, what the Foreign Intelligence Surveillance Act and its amendments actually provide. It reached conclusions that were not necessarily supported in what was before it, which is rather unpredictable and I think it took many people by surprise. Now there are several other cases pending that would impugn the Privacy Shield, the standard contractual clauses as well, and so that adds a measure of unpredictability into what has otherwise been a flexible regime.

The Privacy Shield came out of the *Schrems* case, and the Privacy Shield is a positive example of a mechanism that allows for cross-border flow of data. But I do not think it is in the interest of the FTC or companies to negotiate one hundred different Privacy Shields with every different country that wants to declare adequacy or have a restriction in place.

I would cite the APEC cross-border privacy rule system as a good example of a regime that is flexible enough to accommodate countries like Mexico, in which data protection is a fundamental right, and countries like the United States, in which it is not. And although you mentioned that APEC is really a system that was crafted to respect economic concerns rather than fundamental

rights, I would submit that it is flexible enough to do both. It is an accountability-based system, which, in the APEC system, just to give a brief overview, the APEC economies have to approve participation of an economy, and the economy has to designate its regulator, which in the case of the United States is the FTC, to show that there is enforcement of data protection rules, to show that someone is monitoring this. Then APEC has to approve an accountability agent, a third party who looks at the companies, looks at the transfers of data, and determines that they are in accord with the agreement. Then the accountability agent evaluates companies. Companies have to sign up to participate in the system. Only a handful of companies—twenty-some, perhaps—have been approved at present. And the accountability agent monitors them while the FTC monitors the accountability agent and the companies themselves, and the APEC economies monitor each other. There is an overarching system of institutions holding each other accountable.

The question is, could we take a system like this and make it even more global? It has been proposed that perhaps even the APEC system could transcend the APEC and be given either its own secretariat or some kind of system in which it could be open to countries that are not APEC participating economies, and that, I think, is a very interesting question for international trade lawyers, for policy people, for governments to consider. And, in fact, the APEC system and the EU are looking at ways in which their mechanisms for data transfer can become interoperable.

I will stop there. Thank you.

Paul Schwartz

Thank you so much. Kurt.

Remarks by Kurt Wimmer*

doi:10.1017/amp.2019.126

Thank you, Paul. It is really an honor to be here, so thank you so much to the family and to ASIL. I also am honored that my mentor and friend, Peter Trooboff is here in the front row. No pressure on me at all. No pressure. But really, Peter is the most intellectually generous lawyer I have ever known, so it is wonderful that he is being honored today.

Like Hugh, I am not a trade lawyer, so I thank you, Kristina, for this incredible education about the conflict between international trade law and data protection law, and your paper is really a tour de force and it is really, really helpful as a resource. It struck me, when I started thinking through these issues, though, that there are many areas where there are conflicts between economic values like international trade and human rights, and data protection is not the only issue where there is a human rights issue that collides with a potential free trade right. Restrictions on media distribution, for example, can have free expression impacts. Even things such as international trade in wheat and soybeans can have real human rights impacts in countries where those rights are restricted. I grew up in the center of this country where those sorts of trade decisions have a real human impact.

It will not surprise you to know, as a practitioner of data protection law, that the restrictions on transfer of data have really been a thorn in my side, and in my clients' sides, for many years, and often result in restrictions that do not seem to advance the notion of data protection as protecting fundamental human rights. Hugh mentioned HR data, which is a great example of an area where multinational companies are really striving to do the right thing, working to manage their data in a really effective way, but are having difficulty because of these restrictions on the removal of data from a particular economic entity.

* Covington & Burling LLP.

I do come to a nuanced view on this. I do agree with Kristina that the EU has every right, as an economic organization, as a polity, to come up with a law like the GDPR that protects privacy as a human right. The question I have is whether certain aspects of the EU's data protection regime are really needed or are redundant. The prime problem with the GDPR, and with the '95 directive before it, was this notion that you cannot remove the personal data of any EU data subject from Europe unless you move it to a country with adequate data protection, with some minor exceptions, which creates a lot of difficulties in terms of dealing with data flows for international companies and businesses.

What I wonder now, going forward, is whether this restriction is really just redundant. If you look at the GDPR there are now new obligations put on controllers, the people who control the data, who collect it, and have the ability to say how it will be used, to make sure that they protect data in the way that they collected it, as it is transferred or as it is processed by service providers or processors. And given that this obligation that has been now placed on the controller, it seems redundant to have this other obligation that provides that there cannot be any movement of that data past the border, except to certain countries that we, the European Union, think are okay, despite the fact that we are holding you, the controller, responsible for making those decisions. And if you really do believe in the GDPR's focus on the data protection obligations of people who collect and process data, then why do you need this additional wall at the border, as it were, and not being able to move data, except to certain countries with adequacy?

Adequacy, it also seems to me, is sort of a failed concept. I am not sure of any other law that would exist for twenty-two years and have only twelve countries qualify, even if you include Guernsey, the Faroe Islands, where sheep outnumber people, and a few other countries that have qualified—Israel, Canada, New Zealand, Argentina, Uruguay. It is a very small number of countries that have been found to be adequate, and then you have countries that have not been able to achieve adequacy that have standards of data protection that meet or exceed those of the EU but simply do not achieve adequacy for technical reasons.

I had to advise a client just yesterday that a certain data protection issue in South Korea might involve jail time. Well, you know, the GDPR is pretty tough, but it does not imprison people. There is nothing that focuses your attention quite like jail time. So, you know, there are tough data protection laws that exist in non-EU countries that have not achieved adequacy, which is a puzzling thing to me.

And then the last piece of the trade issue that I do find very troubling, from a business perspective, is the push for data localization in some countries. And data localization basically means you, as a company, are required to keep any data about data subjects from our country in our country. There is a data localization law in Russia. There is a data localization law that applies to certain companies in China. The EU is going back and forth on data localization.

It is a real problem in my clients' world for many reasons. One is it just destroys the ability of cloud computing to really be beneficial to companies, because cloud computing generally crosses borders, and that is an issue of international law that we deal with all the time, and that the CLOUD Act is also trying to address. It also makes it much more difficult to protect the cybersecurity of your data if you have to have 120 data centers versus ten data centers, where you can really invest in sophisticated systems. If you have to have all these small data centers in every country, that is going to present a significant problem for cybersecurity. And the EU is moving forward on dealing with this as a trade issue, and has come up with, I think, a position that Kristina mentioned in her paper, that strikes me as being quite appropriate, that really there should not be laws that permit countries to require the maintenance of the data of their data subjects in that country, but it has such broad exceptions that it seems the exception can swallow the rule. There is an exception for privacy protection, for example, and arguably any country could make the argument that data localization is a

privacy protective measure because they want to make sure that the data of their citizens is held within their countries.

So, overall, I thought it was a fantastic paper and I appreciated the enormous amount of work that went into it and the education that it gave me, so thank you.

Paul Schwartz

Thank you. Kristina, if you would like to reply to these respondents.

Kristina Irion

Thanks to all of you for the comments. I see that we have a lot of GDPR experts already here, and I find that amazing. But that makes it, of course, a very high-level discussion, and I hope we do not lose the audience. I will try to explain a few things or just react, but I cannot comment on everything. Many good and valid points made.

What is fundamental in the GDPR? As I said, I also do not want to defend every half sentence in this law. It has ninety-nine articles, and my boss, Nico van Eijk, already says there was somebody afraid to make Article 100. It is a really voluminous and difficult legal instrument that requires a lot of expertise to actually handle and implement it, and this is never good when you make public policy because it makes it difficult to apply. We want that this law is applied by many small companies that do not have such a huge compliance capacity. I am totally on that page. It should rather have been a layered regulation that has a baseline level where everybody has an easy entry, similar to traffic rules. And then the more sophisticated data processing gets, the more you can also expect in terms of obligations and compliance effort and so on.

I am totally on your page, but now we have the GDPR. It is a product of a ten-year-long legislative process in the EU, different talking heads that tried to make law together. Now we have this law and that is it. We have to live with it for a while, at least. What is fundamental? Everything now. But I also find it difficult sometimes to argue in favor of this complexity that is a problem.

And I also see that you completely understand the transfer. The adequacy decision is like the best status a country can have to receive data from the EU, because it basically gives a presumption of legality of this data transfer and you, as a company, you do not have any headache anymore about getting this data, or you do not need to make any extra compliance effort because your law already has what the EU anyway would require. This is like a convenience thing. In practice, it is not so important, first of all because the EU never really issued many adequacy decisions, there is such a bottleneck to get an adequacy decision.

I would say 90 percent of all the data flows are actually not flowing under the adequacy regime but something else, mostly contractual safeguards. And when you go back now to this example of Kurt, and also from you, Hugh, on the human resource data that international companies have to share, they do not use adequacy or anything like this. For this they can use binding corporate rules, which is like a contract that binds the different branches of this organization to certain standards and then the data of these employees flows happily, and there are even data protection rules attached to it.

There are really different mechanisms, and together this is also an important overflow mechanism, because if they would only rely on the adequacy regime, the system would be seriously broken. How important is adequacy in practice? Less than we think. We all talk about it but in practice it does not matter that much.

And I agree very much with the two points that Lisl has made, and that is predictability and interoperability. The law should be predictable, and obviously an app developer somewhere in the world, who has a brilliant idea, and puts it in some app store, in the end, how does this person

know that there is this rather voluminous GDPR in the EU that he would need to apply because he also wants to target EU citizens? Of course, she does not know that. That is normal. But we should also not underestimate that our online ecosystem is already structured by rather large platforms, and we have the app stores, and we have operating systems, and we have device manufacturers that are using their platform position to have contracts with app developers and end users.

So, in fact, there is a way of at least disseminating some of the requirements also to a small app developer if this is part of entering a platform, because also a platform needs to make sure that what it dissipates applies with certain standards. And we are seeing that increasingly happening, and we have also seen a regulatory expectation that platforms have an important role to play in diffusing these standards. Very important.

And for the interoperability I also would sometimes think—and you have here so many good examples given that the world is having very different ways of regulating data. But for much of the substance it does not create conflicts of law. Just think of it more like different levels. There is baseline protection in some countries and then there are higher levels of protection in other countries. As long as the different laws do not contradict each other you can actually work with it much better than when you have clear conflicts of laws, when the laws have different requirements and the provider can either do it wrong here or disappoint another legal order. This kind of horizontal interoperability you can achieve practically very easily. Take the choice requirement that is sometimes here in the United States, where people have to opt out if they do not want something. In the EU, people have to opt in. But what matters is that there is a control element of the opt-out or the opt-in and you can make a different default for EU citizens, and if you want to be very nice, with U.S., you can also use this default for them. But in the end, they only need an opt-out. You can actually put these variations in there.

And the very last, is when you look at the big picture, like really global, then we see at the moment three different systems running, and some of them are gaining strength. Let us say the United States and a number of countries want the free flow of data—free flow, I call it, this system. EU and a number of other regions, also some Asian countries, they want regulated data flow. And then we have this other bloc, which is China and Russia and a few very strict countries that have a control approach, without much flow actually. Data has to stay, it cannot travel.

If I see strategically, like in the long run, if the free flow people and the regulated flow people could strike a good alliance then there would be enough clout to actually push back the control. But we can also continue and rip each other apart and that will just change the dynamics to the favor of the control.

Thank you very much.