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.

Downloaded from https://www.cambridge.org/core. IP address: 18.234.236.14, on 19 Apr 2019 at 03:58:28, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/amp.2019.123

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

Downloaded from https://www.cambridge.org/core. IP address: 18.234.236.14, on 19 Apr 2019 at 03:58:28, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/amp.2019.123

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

Downloaded from https://www.cambridge.org/core. IP address: 18.234.236.14, on 19 Apr 2019 at 03:58:28, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/amp.2019.123

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.

Downloaded from https://www.cambridge.org/core. IP address: 18.234.236.14, on 19 Apr 2019 at 03:58:28, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/amp.2019.123

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.

Downloaded from https://www.cambridge.org/core. IP address: 18.234.236.14, on 19 Apr 2019 at 03:58:28, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/amp.2019.123

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,

Downloaded from https://www.cambridge.org/core. IP address: 18.234.236.14, on 19 Apr 2019 at 03:58:28, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/amp.2019.123

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.

Downloaded from https://www.cambridge.org/core. IP address: 18.234.236.14, on 19 Apr 2019 at 03:58:28, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/amp.2019.123