EU Law on Cross-Border Flows of Personal Data in a Global Perspective

Irion, K.

Publication date
2018
Document Version
Author accepted manuscript
Published in
Gyeongje Gyuje wa Beob = Journal of Law and Economic Regulation

EU LAW ON CROSS-BORDER FLOWS OF PERSONAL DATA IN A GLOBAL PERSPECTIVE

Kristina Irion[*]

Abstract

This year's conference of the Center for Law and Public Utilities (CeLPU) explored the Law's Evolution and Response to Data-Driven Innovation. As a topic it connects the rise of data-intensive businesses and the global flow of data with law's responses to these phenomena. It rekindles notions of countries' jurisdiction and sovereignty, human rights and the corresponding need for the interoperability of legal systems. One legal sub-system that springs to our mind concerns the protection of individuals' privacy and personal data.

Personal data is peculiar in the way it brings the dignity of a human being together with valuable economic properties. This ambiguity is the reason why personal data protection and data flows are closing in on each other in an increasingly connected and data-driven society. The EU has a key role to play in the global governance of privacy and in particularly regarding the protection of personal data. This role accrues to the EU by virtue of its external relations with third countries stretching over two policy areas for which it has exclusive competences: international transfers of personal data and external commercial policy.

This paper aims to convey EU data protection law and reflect its approach to cross-border flows of personal data in a global perspective. The argument passes through four consecutive stages: first, we will lay the necessary background in the constitutional and regulatory trajectory of personal data protection in the EU. We will proceed to revisit EU governance of cross-border flows of personal data to third countries that will help us to understand the logic of adequacy that is central to EU fundamental rights approach. Next we are going to turn our attention to the impeding stand-off between free trade agreements and domestic data protection law before we explain how the EU plans to regain consistency between its external trade and data protection policies. Last but not least, we will resolve some of the tension between cross-border digital trade and EU-style personal data protection with recourse to a study from the Privacy Bridges project family.

Grounded in the understanding of how deeply entrenched the protection of privacy and personal data have become in EU law and jurisprudence, this paper sets out to establish realistic coordinates for cross-border flows of personal data. We conclude that the EU will throw its weight behind its brand-new General Data Protection Regulation when negotiating digital trade and cross-border data flows. Building privacy bridges could offer a more realistic and constructive path forward that is to a certain extent respectful of local differences while focusing efforts on practical solutions that deliver for individuals and companies alike.

---

[*] Assistant Professor, Institute of Information Law (IViR) at the University of Amsterdam.
I am grateful to Professors Won-Woo Lee and Mellissa Hye-Sun Yoon as well as the participants of the 17th International Conference "The Law's Evolution and Response to Data-Driven Innovation," hosted by the Center for Law & Public Utilities (CeLPU), School of Law, Seoul National University, and Richardson School of Law, University of Hawaii, Honolulu, September 7, 2018.

EU LAW ON CROSS-BORDER FLOWS OF PERSONAL DATA IN A GLOBAL PERSPECTIVE

Kristina Irion

Contents

I. Introduction

This year's conference of the Center for Law and Public Utilities (CeLPU) is exploring the Law's Evolution and Response to Data-Driven Innovation. This subject connects the rise of data-intensive businesses and the global flow of data with law's responses to these phenomena. It rekindles notions of countries' jurisdiction and sovereignty, human rights and the corresponding need for the interoperability of legal systems. One legal sub-system that springs to our mind concerns the protection of individuals' privacy and personal data. Domestic data protection laws regulating the collection and use of personal data stand in a stark contrast with industry's logic of data accumulation, unlimited exploitation and unrestricted flow.

Personal data is peculiar in the way it brings the dignity of a human being together with valuable economic properties.[2] Contemporarily, individuals generate a personal data trail as a by-product of their multifarious online activities, which largely exceeds the personal information they actively volunteer in online transactions. Thanks to the 'smart' everything - from phones to watches, household appliances, cars and entire cities - our movements and activities get registered, even when we are offline.[3] What springs to mind is an analogy to silkworms that produce as a byproduct a raw silk thread which we use to make a luxury cloth.[4] In a similar vein, each data thread is processed for potentially spinning money of it with profiling, personalization and online advertisement.

Cross-border data flows are moreover at the heart of today's global digital economy. A 2016 report of McKinsey Global Institute (MGI) purports that cross-border data flows now exert a larger impact on the global gross domestic product (GDP) than trading goods.[5] Conflicting public interests and objectives that could decelerate the positive feedback loop of global data flows on international trade, growth and welfare become increasingly hard to justify. Especially as digital trade flourishes with the free flow of data, the role of privacy and personal data protection in the governance of data flows is becoming contested in for a, such as international trade law.

Finally, the logic of accumulation is further exacerbated by the prominent role data is bound to play in training algorithms, underpinning machine learning and enhancing artificial intelligence (AI) systems. This link, it has been argued, translates into a firm's competitive edge and even countries can use it strategically.[6] The Villany report outlining the cornerstones of a French and EU AI

---

[2] Beate Roessler, 'Should Personal Data Be a Tradable Good? On the Moral Limits of Markets in Privacy' in Beate Roessler and Dorota Mokrosinska (eds), *Social Dimensions of Privacy: Interdisciplinary Perspective* (Cambridge: Cambridge University Press 2015).

[3] Marie-Pierre Granger and Kristina Irion, 'The Right to Protection of Personal Data: The New Posterchild of European Union Citizenship?' in Sybe de Vries, Henri de Waele and Marie-Pierre Granger (eds), *Civil Rights and EU Citizenship* (Edward Elgar Publishing 2018), 279-302, 279.

[4] Analogy adapted from Chris Marsden and Ian Brown, *Regulating Code: Good Governance and Better Regulation in the Information Age* (Cambridge MA: MIT Press, 2013).

[5] McKinsey Global Institute, 'Digital Globalization: The New Era of Global Flow' (2016) <http://www.mckinsey.com/~/media/McKinsey/Business Functions/McKinsey Digital/Our Insights/Digital globalization The new era of global flows/MGI-Digital-globalization-Full-report.ashx>.

[6] Avi Goldfarb and Daniel Trefler, 'AI and International Trade' (2018) <http://www.nber.org/papers/w24254.pdf>; Susan Ariel Aaronson and Patrick Leblond, 'Another Digital Divide: The Rise of Data Realms and Its Implications for the WTO' (2018) 21 Journal of International Economic Law 245 <https://academic.oup.com/jiel/article/21/2/245/4996295>.

strategy goes right into the heart of the debate stating that "[d]ata is a key competitive advantage in the global AI race" and recommends a data policy that takes into account AI requirements.[7] While access to data features prominently in countries national AI strategies, regulating personal data can be leveraged distinctively in order to foster digital trust and acceptance of human-centric AI systems.

This paper aims to convey EU data protection law and reflect its approach to cross-border flows of personal data in a global perspective. Grounded in the understanding of how deeply entrenched the protection of privacy and personal data have become in EU law and jurisprudence, this paper sets out to establish realistic coordinates for cross-border flows of personal data. In doing so the paper covers how EU policy governs cross-border flows of personal data under data protection law and external trade. In a global perspective the EU approach is certainly very demanding but not impossible to reconcile with other countries' approaches to the protection of personal data.

The argument passes through four consecutive stages: first, we will lay the necessary background in the constitutional and regulatory trajectory of personal data protection in the EU. We will proceed to revisit EU governance of cross-border flows of personal data to third countries that will help us to understand the logic of adequacy that is central to EU fundamental rights approach. Next we are going to turn our attention to the impeding stand-off between free trade agreements and domestic data protection law before we explain how the EU plans to regain consistency between its external trade and data protection policies. Last but not least, we will resolve some of the tension between cross-border digital trade and EU-style personal data protection with recourse to a study from the Privacy Bridges project family.

II. EU's approach to personal data protection

Since the mid-nineties the European Union (EU) has established its reputation as an international champion of personal data protection legislation when passing the Data Protection Directive.[8] The EU comprehensively regulates the handling of personal data thereby aiming for a high level of protection. Owing to the EU's market integrating function, the twin purpose of the legislation has always been to guarantee both the free movement of personal data in the EU internal market and the protection of individuals' fundamental rights. In order to fully comprehend the EU approach, it is necessary to trace the trajectory of personal data protection from a regulatory subject to a full-blown fundamental right.

1. Constitutionalizing the right to the protection of personal data

When in 2000 the EU institutions officially codified the fundamental rights and freedoms of EU citizens in the Charter of Fundamental Rights (the Charter) it marked also the birth of the right to the protection of personal data made.[9] From 2000 to 2009, the Charter had not been legally binding until Article 6 (1) of the Treaty on European Union incorporated the Charter into EU primary law. The

[7] Cedric Villani, 'For a Meaningful Artificial Intelligence: Towards a French and European Strategy' (2018) <https://www.aiforhumanity.fr/pdfs/MissionVillani_Report_ENG-VF.pdf>.

[8] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] Official Journal of the European Union L 28/31 (no longer in force).

[9] Charter of Fundamental Rights of the European Union, 2010 Official Journal of the European Union C 83/02.

entry into force of the Charter marks an important development in EU law which is now fully grounded in its own fundamental rights system.

The right to the protection of personal data is a contemporary fundamental right that has been elevated to the classical canon of fundamental rights in the European constitutional tradition. Not betraying its regulatory origins Article 8 of the Charter must be considered an atypical provision in many respects:

Article 8
Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

First of all, it provides for an autonomous right to the protection of personal data, emancipating itself from the classical fundamental right to privacy. This is distinctive of the EU approach to data protection, and the full implications of this separation of data protection from the right to private life are yet to be explored. Second, it prescribes an institutional requirement of supervision by an 'independent authority', "which entrenches continued and professionalized data privacy bodies in the EU."[10] Institutions of data protection are a means of "redistribution of social and legal powers"[11] that have been remarkably successful in reinforcing individual positions of rights in EU legislation and institutional practices. Moreover, the successful invocation of the 'constitutionalized' right to data protection in litigation before EU and national courts amplifies its position in the EU fundamental rights' framework.

2. The Court of Justice's special regard for the right to the protection of personal data

Only the Court of Justice of the European Union (CJEU) can review the legality of legislative and other acts of EU institutions and has jurisdiction to invalidate those acts. Moreover, the court's interpretations of EU law are binding inasmuch as EU primary law, such as the Charter, is. The frequency with which the CJEU rules on the interpretations of the rights to privacy and data protection in EU law is constantly accelerating. The increasing case-load can certainly be attributed to the contemporary relevance of these issues in a data-driven society which leads to more cases being referred to the CJEU. However, contrary to earlier case-law, which had a rather limited effect, the recent CJEU decisions have gained prominence for their principle contribution to EU law.

When it comes to data protection, "the CJEU has displayed a welcoming and encouraging approach, which contribute to further reinforce the protective EU framework."[12] A number of

[10] Granger and Irion (n 3).
[11] Stefano Rodotà, 'Data Protection as a Fundamental Right' in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (Springer Netherlands 2009).
[12] Granger and Irion (n 3).

indicators and anecdotal evidence can be invoked in support of the Court's 'special regard' for the right to the protection of personal data since the Charter was accorded binding legal value in 2009:[13]

> "First, the well above average frequency with which the Court sits as a 'Grand Chamber' in data protection cases signals their importance in the eyes of the Luxembourg judges. Second, the unusual readiness with which the Court annulled EU acts found to disproportionately restrict the right protected by Articles 8 of the Charter, also suggests that data protection is 'different' from other rights, for which the Court has shown greater deference to EU law-makers. Finally, the quality and rigor of the Court's reasoning in data protection cases, which contrasts with the brusque manner in which it sometimes brushes away other human rights arguments, suggests there is a strong consensus within the Court in support of that cause."[14]

In the pre-Charter era, the Court was still held to favor the free movement of personal data in the light of which individuals' data protection rights were interpreted. The Court would for example consider the free flow of personal data in the EU internal market as the principle aim of data protection legislation.[15] As of 2010, after the Charter was accorded binding effect, the CJEU started to ground its legal argument directly on the Charter. In two landmark rulings the Court was calling for "effective and complete protection"[16] and a "high level of protection"[17] of the fundamental rights to privacy and personal data protection. As we concluded elsewhere, the data protection portfolio has offered the Court a unique opportunity to boost its own legitimacy and expand its review powers.[18] In the process, the it has positioned itself as a guardian EU citizens' fundamental rights, and has demonstrated that EU's highest court could live up to its constitutional mandate.

3. The General Data Protection Regulation in force

The increased volume, variety and velocity of 'big data' applications called for an upgrade of the EU framework on the protection of personal data. Beginning in 2012, the Commission initiated a major reform of the legislative framework that would overcome the persistent fragmentation of the internal market caused by divergent national implementations of the 1995 Directive, modernize data protection law, and guarantee a better protection of individuals' fundamental rights. Just recently this major reform has been accomplished when the General Data Protection Regulation (GDPR) entered into force in May 2018 which as an EU Regulation will be binding and directly applicable in the member states.[19]

---

[13] Kristina Irion, 'A Special Regard: The Court of Justice and the Fundamental Rights to Privacy and Data Protection' in U Faber and others (eds), *Gesellschaftliche Bewegungen - Recht unter Beobachtung und in Aktion: Festschrift für Wolfhard Kohte* (Nomos 2016).

[14] Granger and Irion (n 3).

[15] See e.g. CJEU, joined cases C-465/00, C-138/01 and C-139/01 (*Österreichischer Rundfunk*), judgment of 20 May 2003, [2003] E.C.R. I-04989, para. 70.

[16] CJEU, case C-131/12 (*Google Spain SL and Google Inc. v AEPD and Mario Costeja González*), judgment of 13 May 2014, ECLI:EU:C:2014:317, para. 53.

[17] CJEU, case C-362/14 (*Maximillian Schrems v Data Protection Commissioner*), judgment of 6 October 2015, ECLI:EU:C:2015:650, para. 39.

[18] Granger and Irion (n 3).

[19] Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, Official Journal of the European Union L 119/1-88 (hereinafter: GDPR).

By and large, the GDPR preserved the regulatory approach, first adopted in its predecessor, tying-in the high level of protection of personal data with the free movement thereof in the internal single market. In its substance, the GDPR comes with a range of improvements, clarifications and a few novelties. For example, to mention just a few highlights, new obligations on entities controlling personal data to conduct data protection impact assessments and to innovate pursuant to the principles of privacy by design and default. Incumbent to a strict standard of accountability organizations must thus assess their processing to determine risks and precautions, and they are therefore forced to take individuals' rights and interests into account before processing their personal data.

Ironically, certain regulatory innovations introduced by the GDPR to cope with technological advancement and the data-driven economy appear less capable of yielding the protection desirable for individuals. As we have argued elsewhere, for example the specialized provisions on automated decision-making and profiling in the GDPR may not correspond with the practice of big data and algorithmic decision-making.[20] Article 22 of the GDPR appears to project that for profiling and automated decision-making the input and the output data relate to identical individuals, which is in reality not that straightforward. Rather it is the generic key principles and procedural rights of individuals, which have been established substance of the EU data protection law since its inception, that are more potent to mitigate risks for individuals' personal autonomy.[21]

Probably the most interesting innovation, also when it comes to its pull as an international 'gold standard', concerns the territorial scope of the Regulation. Indeed, the GDRP applies externally, to protect all individuals located in the EU and whose personal data is gathered in the course of online transactions or in the context of monitoring their behavior.[22] In these cases EU law superimposes itself on an organization operating outside EU territory yet in control of the collection of personal data from the EU. The justices at the CJEU already paved the way with their expansive interpretation of the territorial scope of EU data protection law in relation to a company with global operations.[23] Such external effect profoundly impacts service providers from outside the EU, who are as of now expected to observe the GDPR in its entirety.

This section traced how the right to personal data protection, now primarily framed as a fundamental right, rather than a market device, has gained a prominent position in the EU constitutional framework. Guaranteed as a Charter right, personal data protection is not only well entrenched in EU primary law but also guarded by EU's highest court and dedicated independent supervisory authorities at EU and member states' levels. This combination has proven a fair amount of resilience during the legislative process leading to the adoption of the GDPR which saw fierce lobbying by the data-intensive industries and associations representing their interests.

III. EU governance of cross-border flows of personal data to third countries

[20] Manon Oostveen and Kristina Irion, 'The Golden Age of Personal Data: How to Regulate an Enabling Fundamental Right?' in Mor Bakhoum and others (eds), *Personal Data in Competition, Consumer Protection and IP Law - Towards a Holistic Approach?* (Springer Press 2018).
[21] ibid.
[22] GDPR, Article 3(2).
[23] CJEU, case C-131/12 (*Google Spain SL and Google Inc. v AEPD and Mario Costeja González*), judgment of 13 May 2014, ECLI:EU:C:2014:317.

The GDPR recognizes that cross-border flows of personal data to third countries are necessary to the expansion of international trade and that the increase in such flows have raised new concerns when it comes to protection of such data.[24] As a matter of principle, transfers of personal data originating in the EU to third countries may only be carried out in full compliance with the provisions in Chapter V of the GDPR. In the eyes of the CJEU these rules are a necessary anti-circumvention mechanism given that EU data protection law read in the light of the Charter could easily be circumvented by transfers of personal data from the EU to third countries for the purpose of being processed in those countries.[25]

1. The adequacy mechanisms in relation to a third country

EU law, for that purpose, relies on a principle differentiation between third countries that ensure an adequate level of protection in their national legal systems and third countries that do not. To be recognized as a country ensuring an adequate level of protection this country must undergo an assessment of its privacy and data protection rules and receive an approval from the Commission (the so-called 'adequacy decision'). This leads to the question of what an 'adequate level of protection' means, and how that is to be appraised. It means following the authoritative interpretation of the CJEU "… that a third country concerned in fact ensures, by reason of its domestic law or its international commitments, a level of protection of fundamental rights essentially equivalent to that guaranteed in the EU legal order..."[26] Decisions on a third country's adequate level of protection are issued by the Commission. Article 45 of the GDPR holds an extensive list of elements that the Commission shall take into account:

a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;
b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and
c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

[24] GDPR, recital (101).
[25] CJEU (*Schrems v Data Protection Commissioner*) (fn. 14), para. 73.
[26] ibid.

The effect of such a decision is a third country is assimilated to the EU internal digital market without the need for the data exporter to provide further safeguards or obtain any authorisation.

Albeit many third countries have transplanted EU data protection principles in their own legislation, so far only a few did receive the desirable adequacy status. To some extent this can be explained with the long and highly customized procedure that findings of adequacy occupy that, depending on the circumstances, can sum up to a few years. So far the Commission granted adequacy status to a total of 12 countries. Apart from a few islands and small territories with strong ties to EU member states, these are Argentina, Canada, Switzerland, Israel, Uruguay and the United States (US) pursuant to the 2016 'EU-US Privacy Shield'. Presently, the Commission finalizes the adequacy finding with Japan,[27] and another adequacy procedure with South Korea is in progress. The impact of data flow arrangements with the EU is arguably considerable, just by looking at the UK which after the 'Brexit' will no longer qualify for receiving personal data from the EU without additional safeguards.

Absent an adequacy finding, transfers of personal data to third countries are only possible subject to appropriate safeguards or one of the subsidiary derogations for specific situations.[28] The meaning of appropriate safeguards are enforceable commitments vis-à-vis individuals that take oftentimes the form of contractual obligations, such as standard contractual clauses and binding corporate rules, but recently also the form of approved codes of conduct and certification mechanisms. Indeed, these measures can overcome bilateral incongruences while keeping wholesale transfers of personal data to third countries not ensuring adequate levels of protection sufficiently restricted.

2. Not if a third country engages in mass surveillance

The EU legal mechanisms for transfers of personal data to third countries have been rightly criticized for being overly formalistic,[29] not to mention that the intricate procedure of the adequacy mechanism has been identified as a bottleneck that may effectively discriminate between third countries in the light of international trade law.[30] The justices at the CJEU, however, seem determined to restrict the international transfer of personal data when this is necessary to protect the fundamental rights of individuals in the EU. In 2015, the CJEU in its landmark *Schrems I* ruling struck down a significant legal basis for transferring personal data from the EU to the US, the so-called 'Safe Harbour', [31] in the wake of the Snowden revelations about blanket mass surveillance of internet communications in the US.[32]

---

[27] European Commission, The European Union and Japan agreed to create the world's largest area of safe data flows, press release, Tokyo, 17 July 2018 <http://europa.eu/rapid/press-release_IP-18-4501_en.htm>.
[28] GDPR Art. 46, 47 and 49.
[29] Christopher Kuner, 'Reality and Illusion in EU Data Transfer Regulation Post Schrems' (2017) 18 German Law Journal 881.
[30] *See* Kristina Irion, Svetlana Yakovleva and Marija Bartl, 'Trade and Privacy: Complicated Bedfellows? How to Achieve Data Protection-Proof Free Trade Agreements' (2016).
[31] CJEU, case C-362/14 (*Maximillian Schrems v Data Protection Commissioner*), judgment of 6 October 2015, ECLI:EU:C:2015:650.
[32] Kristina Irion, 'Accountability Unchained: Bulk Data Retention, Preemptive Surveillance, and Transatlantic Data Protection' in M Rotenberg, J Horwitz and J Scott (eds), *Privacy in the modern age: the search for solutions* (The New Press 2015).

It is important to note that the justices did not examine the content of the 'Safe Harbour' arrangement, but could nevertheless invalidate the Commission's adequacy decision because it did not satisfy the requirements for concluding that a third country ensures an adequate level of protection. The Court holds that the Commission has not based its adequacy decision on a complete assessment of the US legal framework governing the protection of personal data, in particular with regards to disclosure authorities by US entities when they pursue legitimate objectives, such as national security, which was explicitly exempt from the application of the Safe Harbour agreement. The Court then extrapolates from the level of protection in the EU to the legal situation of EU-originating personal data in the US stating that:

> "[…] legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter."[33]

The Court holds that interferences with the rights to privacy and protection of personal data must be limited to what is strictly necessary, and that the right to effective judicial protection must be observed when assessing a third country's legal system. Provided that the court's reasoning is directly based on articles 7 and 8 of the Charter, the CJEU formulates a constitutional baseline that should apply across the board for all transfer mechanisms foreseen in the GDPR. While from an EU law perspective the reasoning of the Court is not setting a new paradigm, its impact on global flows of personal data, however, cannot be overestimated. "To scholars and policy practitioners the ruling did not only strike out one of the legal means to transfer personal data from the EU to the US, but is bound to impact on the legality of exporting EU-originating personal data to third countries in general."[34]

As we content elsewhere, "the confrontation that arises at the triangular interface between protection, export and surveillance of personal data have become emblematic for EU's external relations with the US."[35] In order to replace the invalidated 'Safe Harbor', the so-called 'Privacy Shield' was in short time negotiated between the US government and the European Commission and, following the approval of EU member states, in 2016 enacted.[36] Even though the 'Privacy Shield' has passed its first annual review, two proceedings against its legality are pending at the General Court and the CJEU.[37] Whether personal data exports to the US will withstand the next round of legal scrutiny remains to be seen, yet, also EU's highest court will have to acknowledge the reality of cross-border flows of personal data.

3. EU policy on future adequacy procedures

[33] CJEU, case C-362/14 (*Maximillian Schrems v Data Protection Commissioner)*, para. 94.
[34] Irion (n 13).
[35] Svetlana Yakovleva and Kristina Irion, 'The Interface between Trade and Privacy: Reconciling the European Governance of Personal Data Flows with External Trade' (forthcoming).
[36] Commission Implementing Decision of 12.7.2016 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU-U.S. Privacy Shield <http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf>.
[37] See General Court, case T-738/16 (*La Quadrature du Net and Others v Commission*), pending; CJEU, case C-311/18 (*Facebook Ireland and Schrems*), pending.

In its 2017 Communication on Exchanging and Protecting Personal Data in a Globalised World,[38] the Commission sets out its strategic framework for adequacy decisions as well as other tools for data transfers and international data protection instruments. Internally, a new unit "International data flows and protection" took up work to manage in particular new adequacy assessments vis-à-vis third countries and the forthcoming periodic reviews of existing adequacy decisions.[39]

In relation to the adequacy procedure the Communication recently clarified the criteria which the Commission will take into account when assessing with which third countries a dialogue on adequacy should be pursued:

(i) the extent of the EU's (actual or potential) commercial relations with a given third country, including the existence of a free trade agreement or ongoing negotiations;
(ii) the extent of personal data flows from the EU, reflecting geographical and/or cultural ties;
(iii) the pioneering role the third country plays in the field of privacy and data protection that could serve as a model for other countries in its region; and
(iv) the overall political relationship with the third country in question, in particular with respect to the promotion of common values and shared objectives at international level.[40]

Based on these considerations, the Commission signals more agility to engage with EU's key trading partners in East and South-East Asia, mentioning in particular South Korea. The Communication moreover points out India, depending on its progress in modernizing its data protection laws, as well as countries in Latin America and the European neighborhood.[41] To our reading, "[a] more proactive approach of the EU in opening adequacy procedures would certainly be necessary in order to offer third countries a fair entry point to the procedure and breathe new life into the adequacy mechanisms championed by the EU."[42]

Judging from the experience with Japan the assessment of a third country's legal system and data protection safeguards continues to remain a time-consuming procedure. One the one hand, data-intensive businesses and trade pundits have been very critical about the adequacy approach in general and the low turn-out in terms of recognized countries. On the other hand, as a formal mechanism a finding of a third country's adequate level of protection effectively provides for the free flow of personal data between the two economies without further safeguards. The free flow of personal data between the EU and Japan will be significant:

> "This … adequacy arrangement will create the world's largest area of safe transfers of data based on a high level of protection for personal data. … With this agreement, the EU and

[38] European Commission, 'Communication from the Commission to the European Parliament and the Council: Exchanging and Protecting Personal Data in a Globalised World COM(2017)7 Final' (2017), section I.3.
[39] GDPR Art. 45 (3).
[40] ibid.
[41] Note that the Commission hosted three official GDPR launch events in Brussels, Delhi (India) and Santiago de Chile on 25 May 2018.
[42] Yakovleva and Irion (n 35).

Japan affirm that, in the digital era, promoting high privacy standards and facilitating international trade go hand in hand."[43]

It is moreover safe a prognosis that adequacy proceedings have become more cognizant of a third country's rules and international commitments about onward data transfers. This follows from the explicit GDPR requirement to assess "rules for the onward transfer of personal data to another third country".[44] For example Japan's participation in the Asia-Pacific Economic Cooperation's (APEC) Cross-Border Privacy Rules[45] has upset the GDPR's logic to restrict onward transfers.[46] As a result the Commission's adequacy decision will likely not permit Japanese companies handling personal data originating from the EU to rely APEC's Cross-Border Privacy Rules for onward transfers. Another area that will likely run against national policy consistency in relation to onward transfers of personal data can arise from the commitments a third country entered into in bilateral or multilateral free trade agreements which are on rise.

IV. International trade law embarking on cross-border data flows

"As digital trade flourishes with the free flow of data," we observe elsewhere, "the role of privacy within international trade law is becoming increasingly controversial."[47] A new generation of trade and investment agreements which have been concluded or are presently negotiated endeavor service liberalization beyond what has been achieved under the General Agreement on Trade in Services (the so-called "GATS-plus" criteria). Such new generation trade agreements endorse digital trade broadly by proposing provisions on cross-border data flows while keeping privacy and data protection as an exception subject to certain trade-conforming requirements.[48]

1. New commitments on the cross-border free flow of information

The US and Korea were concluding the first bilateral trade agreement (KORUS FTA) containing a yet non-binding provision on cross-border free flow of information. The first binding horizontal provision on data flows can be found in the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (TPP-11) signed in 2018, which incorporates by reference the original Trans-Pacific Partnership (TPP) signed in 2016.[49] The TPP requires in article 14.11, para. 2 that:

---

[43] European Commission, The European Union and Japan agreed to create the world's largest area of safe data flows (n 27).

[44] Art. 45 (2)(a) GDPR.

[45] APEC Cross-border privacy rules system at <http://www.cbprs.org/GeneralPages/About.aspx>. See Graham Greenleaf, "Japan joins APEC-CBPRs: Does it matter?" (2016) 144 *Privacy Laws & Business International Report*, 18 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2964499>.

[46] Marija Bartl and Kristina Irion, 'The Japan EU Economic Partnership Agreement: Flows of Personal Data to the Land of the Rising Sun' (2017) <https://www.ivir.nl/publicaties/download/Transfer-of-personal-data-to-the-land-of-the-rising-sun-FINAL.pdf>.

[47] Yakovleva and Irion (n 35).

[48] See Mira Burri, 'The Regulation of Data Flows Through Trade Agreements' (2017) 48 Georgetown Journal of International Law 407.

[49] Comprehensive and Progressive Agreement for Trans-Pacific Partnership between Australia, Brunei, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore, Vietnam, retrieved at <http://dfat.gov.au/trade/agreements/not-yet-in-force/tpp-11/official-documents/Documents/tpp-11-treaty-text.pdf>; note that the new US administration withdrew from the 2016 TPP.

> "[e]ach Party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person."

Unlike existing sectoral provisions related to cross-border data flows,[50] the TPP provision is formulated as a positive horizontal obligation. Any slight connection of transfers to the conducting of business, even if merely incidental, suffices to trigger this provision. As a result, any restriction of transfers of personal data in a party's domestic laws might lead to a violation of this provision that has to be justified under a specific exception provided for in the agreement:

> "Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure: (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and (b) does not impose restrictions on transfers of information greater than are required to achieve the objective."[51]

These new rules have not been put to a test yet, however, consider that Japan, being a party to the TPP-11, would have to meet this test when its national data protection law causes a restriction on cross-border data flow. Our legal assessment of how an adequacy mechanism, as is practiced in both the EU and Japan, would fare in light of a trade-law exception concluded that the justification could not be met.[52] Such nourishes the assumption that committing to the cross-border movement of personal data in free trade agreement may lead to an irreconcilable conflict with domestic data protection laws that place conditions on cross-border transfers of personal data.

2. The new EU position on cross-border data flows

The quest for cross-border data flows has also surfaced in bilateral and multilateral trade agreements the EU has entered into or is currently negotiating. The Commission's 2015 trade and investments strategy affirms that the free flow of data across borders as an offensive interest for the EU.[53] The Commission committed 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."[54]

What followed had been an intense inter-institutional dispute on the future direction of EU external trade policy relative to EU data protection law. The EU decided to guard its new GDPR that is specifically designed to defend fundamental rights of its residents against tacit liberalization from trade deals. In spring 2018, the Commission released its position on horizontal provisions on cross-

---

[50] See for example Article B.8 of the Understanding on Commitments in Financial Services and Article 5(c) of the Annex on Telecommunications, both are not a part of the GATS but appendices to the Final Act of the Uruguay Round.

[51] Article 14.11(3) TPP.

[52] See for an analysis Irion, Yakovleva and Bartl (n 30); Kristina Irion and Svetlana Yakovleva, 'The Best of Both Worlds? Free Trade in Services and EU Law on Privacy and Data Protection' (2016) 2 European Data Protection Law Review 191.

[53] European Commission, *Trade for All: Towards a More Responsible Trade and Investment Policy* (2015) <http://ec.europa.eu/trade/policy/in-focus/new-trade-strategy/%5Cnhttp://trade.ec.europa.eu/doclib/docs/2015/october/tradoc_153846.pdf>.

[54] ibid.

border data flows and personal data protection in EU trade and investment agreement.[55] The Commission started to introduce its new position in all bilateral trade agreements it is currently negotiating with third countries.

The position carries an unconditional counter-balancing provision for national measures in the interest of the protection of personal data:

Article B
Protection of personal data and privacy

1. Each Party recognises that the protection of personal data and privacy is a fundamental right and that high standards in this regard contribute to trust in the digital economy and to the development of trade.
2. Each Party may adopt and maintain the safeguards it deems appropriate to ensure the protection of personal data and privacy, including through the adoption and application of rules for the cross-border transfer of personal data. Nothing in this agreement shall affect the protection of personal data and privacy afforded by the Parties' respective safeguards.
3. For the purposes of this agreement, "personal data" means any information relating to an identified or identifiable natural person. […]

Our analysis of the newly found Commission position concludes that in the interest of EU law consistency the preference expressed for the regulatory mechanisms of the GDPR must be welcomed.[56] By trade law standards, the Commission's new position must be considered rather bold provided that the wording goes beyond the existing counterbalancing provisions in the financial and telecommunications sectors in the GATS. Remarkably, the new EU approach to privacy and data protection would even exceed counterbalancing provisions in favor of labor standards, environmental protection and sustainable development in a number of post-GATS trade agreements.

V. Building Privacy Bridges

It would not do justice to the important interests at stake to end this article on the note that free data flows and the protection of privacy and personal data are hopelessly irreconcilable. Not every difference between national law causes conflicts of law, whereby compliance with one country's legal framework inevitably produces a violation of another country's domestic law. Rather it helps to understand that there are different degrees of protection where some countries and regions, such as the EU, would require more than others. In hindsight many bilateral incongruences are manageable from a compliance point of view if one focuses on vertical interoperability.

Precisely this has been the underlying philosophy of the 2015 Privacy Bridges Report, in which a group of international privacy experts put forward ten proposals (so called 'privacy bridges') to foster stronger international collaboration and advance privacy protection for individuals.[57] Varying regulatory requirements stand in sharp contrast, as the report notes, with the global

[55] European Commission, "Horizontal provisions on cross-border data flows and personal data protection," news release of 18 May 2018 <http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=627665>.
[56] Yakovleva and Irion (n 35).
[57] Privacy Experts, 'Privacy Bridges: EU and US Privacy Experts in Search of Transatlantic Privacy Solution' (2015) <https://privacybridges.mit.edu/>.

diffusion of many popular online services and applications. Rather than wait for privacy laws to converge, the Privacy Bridges Report argues in favor of practical measures to advance strong privacy values "in a manner that respects the substantive and procedural differences' between national privacy laws."[58] The second privacy bridge called for practical solutions for enhancing user control that operate "regardless of jurisdiction, citizenship, and location of data":

> "Users around the world struggle for control over their personal information. This bridge calls on technology companies, privacy regulators, industry organizations, privacy scholars, civil society groups and technical standards bodies to come together to develop easy-to-use mechanisms for expressing individual decisions regarding user choice and consent. The outcome should be usable technology, developed in an open standards-setting process, combined with clear regulatory guidance from […] regulators resulting in enhanced user control over how data about them is collected and used."[59]

In a follow-up report, to which the author contributed, we propose four measures which can be combined to achieve cross-national interoperability: 1) consolidation of legal requirements, 2) customization of default-settings, 3) voluntary upgrading of privacy controls and 4) the application of privacy by design approaches.[60] Below we will reproduce how report approaches user controls that can, on the one hand, respect differences of national privacy laws, and, on the other hand, produce interoperability and constructive interfaces between them:

> "The first measure, i.e., the consolidation of legal requirements, means to consolidate, as much as possible, common denominators of various privacy laws with the intention to achieve compliance across legal regimes. To this end it does not yet matter whether applicable privacy laws mandate users' prior permission or consent to the collection and use of personal data. What matters is whether there is a user control requirement at all. Different jurisdictions around the world will often coincide about mandating user control over the collection and use of personal data."[61]

> "Under the second measure, customizing default-settings of a given user control mechanism can accommodate differences between privacy laws to some extent. If a particular privacy law requires an expression of consent or a permission to the collections and use of personal data, such legal default should be appropriately reflected in the default-settings. Simultaneous compliance with the law of a provider's country of origin and the country of a user can in many instances be accomplished via the choice of appropriate defaults."[62]

> "A third measure, which we refer to as voluntary upgrading, can be to escalate privacy controls to a stricter legal framework in a situation in which different requirements cannot otherwise be reconciled. Such a voluntary upgrade can nevertheless solve discrepancies to the benefit of users and their trust. Especially consumer-facing services with a global user base may have an interest to excel with their privacy policy beyond what is strictly provided

[58] ibid.
[59] ibid.
[60] Kristina Irion and others, 'A Roadmap to Enhancing User Control via Privacy Dashboards' (2017) <https://www.ivir.nl/publicaties/download/PrivacyBridgesUserControls2017.pdf>.
[61] ibid.
[62] ibid.

for in their country of origin and countries of operation. Voluntary upgrading clearly requires more from stakeholders than a legal compliance attitude."[63]

"The fourth, i.e., the application of privacy by design, is a non-legal measure that aims to reduce the reliance on personal data without compromising the business model or the functionality of a given online service or mobile app. Possible repercussions of internalizing user controls on business models can be mitigated to some extent through technologies that embrace the latest privacy by design solutions. Remaining trade-offs should be balanced against the positive effects of achieving cross-national compliance, reputation and online trust."[64]

This section emphasizes that there are ways to engage with incongruences of countries' data protection laws constructively instead of crying foul over the lack of fully converged legal frameworks and the burden of implementing regulations. After all the values and individual interests at stake merit public and private efforts to guarantee privacy and personal data protection which ultimately buttresses trust in global data flows and human-centric data-intensive technologies.

VI. Conclusions

The EU has been depicted as a normative power that conducts its international relations through a professed rule-of-law based multilateralism.[65] The EU is bound by its founding Treaties to pursue in its international relations the universality and indivisibility of human rights and fundamental freedoms and contribution to their protection, respect for human dignity and for the principles of the United Nations and international law.[66] In EU law, the Charter, in its Articles 7 and 8, guarantees the rights to privacy and the protection of personal data as fundamental rights.

Extrapolating from this, the EU has a key role to play in the global governance of privacy and in particularly regarding the protection of personal data. This role accrues to the EU by virtue of its external relations with third countries stretching over two policy areas for which it has exclusive competences: international transfers of personal data and external commercial policy. The EU has a preference for institutionalized relationships with third countries, emulating strategies that "developed internally as part of its original project of European transnational integration".[67] This may explain why the EU strives for regulatory convergence, mutual recognition and ongoing dialogue.

Personal data protection and data flows are two areas, which are closing in on each other in an increasingly connected and data-driven society. The EU had to adjust its position on cross-border data flows and personal data protection. The new Commission's approach aims to untie EU data protection measures from external trade policy. The division of labor between the GDPR and external trade prioritizes adequacy decisions over trade law to facilitate data flows:

---

[63] ibid.
[64] ibid.
[65] Bart Van Vooren, Steven Blockmans and Jan Wouters, 'The Legal Dimension of Global Governance: What Role for the European Union? An Introduction' in Bart Van Vooren, Steven Blockmans and Jan Wouters (eds), *The EU's Role in Global Governance The Legal Dimension* (Oxford University Press 2013).
[66] Treaty on European Union articles 3(5) and 21.
[67] Grainne de Burca, 'EU External Relations: The Governance Mode of Foreign Policy' in Bart Van Vooren, Steven Blockmans and Jan Wouters (eds), *The EU's Role in Global Governance The Legal Dimension* (Oxford University Press 2013).

> "The EU data protection rules cannot be the subject of negotiations in a free trade agreement. While dialogues on data protection and trade negotiations with third countries have to follow separate tracks, an adequacy decision, including a partial or sector-specific one, is the best avenue to build mutual trust, guaranteeing uninhibited flow of personal data, and thus facilitate commercial exchanges involving transfers of personal data to the third country in question."[68]

In trade negotiations the Commission is expected to negotiate for an unconditional horizontal exception for a party's respective safeguards on the protection of personal data and privacy as a means to achieve EU law internal consistency. In paying attention to devising a proper counterbalancing provision in its new position the Commission effectively reverses its early stance and accepts the delicacy of excepting the GDPR from its commitments under trade and investment law.

What emerges are two perceived 'gold standards' which could not be more contradictory. The first self-proclaimed 'gold standard' is EU data protection law, now codified as the GDPR, which provides an international example for a high level of personal data protection.[69] The second is the in trade law venues much hyped 'gold standard' for digital trade as championed by the US and other countries prioritizing the liberalization of data flows. The ensuing tension between cross-border data flows and the fundamental rights to the protection of personal data and privacy in the EU will certainly not subside anytime soon.

Future directions in international trade diplomacy should aim to establish realistic coordinates for digital trust in cross-border trade in services which cannot in our opinion be parted from individuals' positions of rights as guaranteed in their countries. Building privacy bridges could offer a more realistic and constructive path forward that is to a certain extent respectful of local differences while focusing efforts on practical solutions that deliver for individuals and companies alike.

Bibliography

Aaronson SA and Leblond P, 'Another Digital Divide: The Rise of Data Realms and Its Implications for the WTO' (2018) 21 Journal of International Economic Law 245 <https://academic.oup.com/jiel/article/21/2/245/4996295>

Bartl M and Irion K, 'The Japan EU Economic Partnership Agreement: Flows of Personal Data to the Land of the Rising Sun' (2017) <https://www.ivir.nl/publicaties/download/Transfer-of-personal-data-to-the-land-of-the-rising-sun-FINAL.pdf>

Burri M, 'The Regulation of Data Flows Through Trade Agreements' (2017) 48 Georgetown Journal of International Law 407

'Commission Implementing Decision of 12.7.2016 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU-U.S. Privacy Shield' <http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf>

de Burca G, 'EU External Relations: The Governance Mode of Foreign Policy' in Bart Van Vooren,

[68] European Commission (n 38).
[69] Nikolaj Nielson, 'GDPR - a global 'gold standard'?', EUobserver of 25 May 2018, retrieved at <https://euobserver.com/justice/141906>.

Steven Blockmans and Jan Wouters (eds), *The EU's Role in Global Governance The Legal Dimension* (Oxford University Press 2013)

European Commission, *Trade for All: Towards a More Responsible Trade and Investment Policy* (2015) <http://ec.europa.eu/trade/policy/in-focus/new-trade-strategy/%5Cnhttp://trade.ec.europa.eu/doclib/docs/2015/october/tradoc_153846.pdf>

——, 'Communication from the Commission to the European Parliament and the Council: Exchanging and Protecting Personal Data in a Globalised World COM(2017)7 Final' (2017)

Goldfarb A and Trefler D, 'AI and International Trade' (2018) <http://www.nber.org/papers/w24254.pdf>

Granger M-P and Irion K, 'The Right to Protection of Personal Data: The New Posterchild of European Union Citizenship?' in Sybe de Vries, Henri de Waele and Marie-Pierre Granger (eds), *Civil Rights and EU Citizenship* (Edward Elgar Publishing 2018) <https://www.elgaronline.com/view/edcoll/9781788113434/9781788113434.00019.xml>

Irion K, 'Accountability Unchained: Bulk Data Retention, Preemptive Surveillance, and Transatlantic Data Protection' in M Rotenberg, J Horwitz and J Scott (eds), *Privacy in the modern age: the search for solutions* (The New Press 2015)

——, 'A Special Regard: The Court of Justice and the Fundamental Rights to Privacy and Data Protection' in U Faber and others (eds), *Gesellschaftliche Bewegungen - Recht unter Beobachtung und in Aktion: Festschrift für Wolfhard Kohte* (Nomos 2016)

——, 'A Roadmap to Enhancing User Control via Privacy Dashboards' (2017) <https://www.ivir.nl/publicaties/download/PrivacyBridgesUserControls2017.pdf>

Irion K and Yakovleva S, 'The Best of Both Worlds? Free Trade in Services and EU Law on Privacy and Data Protection' (2016) 2 European Data Protection Law Review 191

Irion K, Yakovleva S and Bartl M, 'Trade and Privacy: Complicated Bedfellows? How to Achieve Data Protection-Proof Free Trade Agreements' (2016)

Kuner C, 'Reality and Illusion in EU Data Transfer Regulation Post Schrems' (2017) 18 German Law Journal 881

McKinsey Global Institute, 'Digital Globalization: The New Era of Global Flow' (2016) <http://www.mckinsey.com/~/media/McKinsey/Business Functions/McKinsey Digital/Our Insights/Digital globalization The new era of global flows/MGI-Digital-globalization-Full-report.ashx>

Oostveen M and Irion K, 'The Golden Age of Personal Data: How to Regulate an Enabling Fundamental Right?' in Mor Bakhoum and others (eds), *Personal Data in Competition, Consumer Protection and IP Law - Towards a Holistic Approach?* (Springer Press 2018)

Rodotà S, 'Data Protection as a Fundamental Right' in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (Springer Netherlands 2009)

Roessler B, 'Should Personal Data Be a Tradable Good? On the Moral Limits of Markets in Privacy' in B Roessler and D Mokrosinska (eds), *Social Dimensions of Privacy: Interdisciplinary Perspective* (Cambridge University Press 2015)

van Eijk N and others, 'Privacy Bridges: EU and US Privacy Experts in Search of Transatlantic Privacy Solution' (2015) <https://privacybridges.mit.edu/>

Villani C, ‘For a Meaningful Artificial Intelligence: Towards a French and European Strategy’ (2018) <https://www.aiforhumanity.fr/pdfs/MissionVillani_Report_ENG-VF.pdf>

Vooren B Van, Blockmans S and Wouters J, ‘The Legal Dimension of Global Governance: What Role for the European Union? An Introduction’ in Bart Van Vooren, Steven Blockmans and Jan Wouters (eds), *The EU’s Role in Global Governance The Legal Dimension* (Oxford University Press 2013)

Yakovleva S and Irion K, ‘The Interface between Trade and Privacy: Reconciling the European Governance of Personal Data Flows with External Trade’ (2019 forthcoming).