doi:10.1017/aju.2019.81

SYMPOSIUM ON THE GDPR AND INTERNATIONAL LAW

TOWARD COMPATIBILITY OF THE EU TRADE POLICY WITH THE GENERAL DATA PROTECTION REGULATION

Svetlana Yakovleva[*] *& Kristina Irion*[**]

The European Union's (EU) negotiating position on cross-border data flows, which the EU has recently included in its proposal for the World Trade Organization (WTO) talks on e-commerce, not only enshrines the protection of privacy and personal data as fundamental rights, but also creates a broad exception for a Member's restrictions on cross-border transfers of personal data.[1] This essay argues that maintaining such a strong position in trade negotiations is essential for the EU to preserve the internal compatibility of its legal system when it comes to the right to protection of personal data under the EU Charter of Fundamental Rights[2] (EU Charter) and the recently adopted General Data Protection Regulation (GDPR).[3]

EU Regulation of Cross-Border Transfers of Personal Data

The GDPR impacts international flows of personal data and therefore cross-border trade in services in two distinct ways. First, Chapter V regulates the transfer of personal data outside of the European Economic Area (EEA).[4] The EU stands out for its commitment to the sui generis protection of personal data as a fundamental right, which stretches beyond the fundamental right to privacy.[5] The export of personal data to third countries is subject to formalities that aim to provide a safety valve for the EU's high level of personal data protection so that it cannot be rendered meaningless by the transfer of personal data to so-called "data havens." Personal data originating in the EEA can be transferred without any further safeguards pursuant to a formal finding from the EU of an adequate level of protection in the receiving country (often called an "adequacy finding"). In the absence of an adequacy finding, the GDPR provides a catalogue of alternative transfer mechanisms, all of which harness private

* *Ph.D Candidate, Institute for Information Law (IViR), University of Amsterdam; Lawyer, De Brauw Blackstone Westbroek (Amsterdam).*

** *Assistant Professor, Institute for Information Law (IViR), University of Amsterdam.*

[1] *EU Proposal for WTO Disciplines and Commitments Relating to Electronic Commerce*, EUR. COMM'N COMMC'N, INF/ECOM/22, paras. 2.7–2.8 (Apr. 26, 2019).

[2] Charter of Fundamental Rights of the European Union arts. 7 and 8, 2000 O.J. (C 364) 1 (Dec. 18, 2000) [hereinafter EU Charter].

[3] Regulation (EU) 2016/679 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 (General Data Protection Regulation), 2016 O.J. (L 119) 1 [hereinafter GDPR].

[4] The EEA is an extension to the EU internal market by three European Free Trade Association states: Iceland, Liechtenstein, and Norway.

[5] EU Charter, *supra* note 2, arts. 7 and 8.

law to incorporate appropriate safeguards in connection with a personal data transfer. Standard contractual clauses are the most widely-used mechanism in practice.

Second, the GDPR's new territorial scope of application is no longer confined to the processing of personal data by entities established in the EU. In a much-noticed legal adaptation to the prevalence of foreign online service providers, the GDPR applies directly to cross-border transactions involving personal data of individuals in the EEA even if the entity in charge operates from outside the EEA.[6] This scope of application profoundly impacts suppliers of goods and services from outside the EEA, who must comply with the GDPR in its entirety. These entities, moreover, must designate a representative in the EEA to ensure compliance with the GDPR.

The regulation of personal data transfers outside the EEA primarily functions as an anti-circumvention mechanism. This understanding was confirmed by the Court of Justice of the EU (CJEU) in the *Schrems* judgment.[7] Likewise, the new territorial scope of application is essentially motivated by the aim of ensuring "that natural persons are not deprived of the protection to which they are entitled,"[8] retaining as a jurisdictional touchpoint that the rights of individuals in EEA territory are affected when their personal data are processed by non-EEA entities. Note in this context that the EU Charter protects the rights to privacy and to the protection of personal data not only as an end in itself, but also as a proxy to safeguarding human dignity, democracy, and personal autonomy in the age of "surveillance capitalism."[9]

Mutual Inconsistency Between the GDPR and the GATS

From an international trade law perspective, the GDPR rules on cross-border personal data transfers could violate the EU's non-discrimination commitments under the General Agreement on Trade in Services (GATS) in several ways. For example, one could argue that the use of adequacy findings violates the principle of most-favored-nation treatment by giving disparate treatment to transfers of personal data to countries that have received an adequacy finding, as opposed to those that have not.[10] In addition, the EU arguably applies a double standard in relation to surveillance conducted by its own member states[11] vis-à-vis non-EEA countries, notably the United States, which could be inconsistent with the EU's national treatment commitments.

The GATS contains an exception for domestic privacy and data protection rules in Article XIV(c)(ii). However, there is a risk that the potential violations described in the preceding paragraph cannot be justified under this exception.[12] The "necessity test"—the core of the exception—has been particularly hard to pass even in its more lenient interpretation.[13] It requires that a GATS-inconsistent regulation should be the least trade-restrictive of all "reasonably available" alternatives. One can argue, for example, that the adequacy approach is not the "least

[6] GDPR, *supra* note 3, art. 3(2).

[7] *See* Case C-363/14, Schrems v. Data Protection Commissioner, ECLI:EU:C:2015:650, para. 73 (Eur. Ct. Justice, Oct. 6, 2015) [hereinafter Schrems]; *see also* GDPR, *supra* note 3, art. 44.

[8] GDPR, *supra* note 3, recital (23).

[9] *See* Shoshana Zuboff, *Big Other: Surveillance Capitalism and the Prospects of an Information Civilization*, 30 J. Info. Tech. 75, 83 (2015).

[10] *See, e.g.,* Kristina Irion et al., *Trade and Privacy: Complicated Bedfellows? How to Achieve Data Protection-proof Free Trade Agreements* 28–30 (Study commissioned by BEUC et al., Amsterdam, Institute for Information Law (IViR), July 13, 2016).

[11] Peter Swire, Testimony in Irish High Court Case Data Protection Commissioner v. Facebook Ireland Limited & Maximillian Schrems, 1-1, 1-2.

[12] Svetlana Yakovleva & Kristina Irion, *The Best of Both Worlds - Free Trade in Services and EU Law on Privacy and Data Protection*, 2 Eur. Data Prot. L. Rev. 191, 198–99, 206–07 (2016).

[13] *See, e.g.*, Ingo Venzke, *Making General Exceptions: The Spell of Precedents in Developing Article XX GATT into Standards for Domestic Regulatory Policy*, 12 German L.J. 1111, 1116–37 (2011).

https://doi.org/10.1017/aju.2019.81 Published online by Cambridge University Press

trade-restrictive," as other less trade restrictive data transfer mechanisms, such as those practiced by Canada and certain Asia Pacific Economic Community countries, are "reasonably available" to the EU.[14]

From an EU law perspective, restrictions on cross-border transfers of personal data are constitutionally required to guarantee a high level of protection of the fundamental rights to which natural persons are entitled. Following a classical human rights review under the EU Charter, the EU can adjust its personal data transfer rules to comply with the GATS only to the extent it is "strictly necessary" to meet objectives of general interest of the EU or to protect the rights and freedoms of others.[15] In the context of cross-border data transfers, "strict necessity" requires, in particular, that legislation or an international agreement allowing personal data transfers outside the EEA lay down clear and precise rules on the access of foreign governments to personal data and ensure the existence of an effective judicial remedy for individuals.[16] The adequacy approach—the most questionable from a trade law perspective—is thus, in theory, the only personal data transfer mechanism that fully complies with these constitutional requirements. It requires the European Commission to evaluate a foreign country's rule of law, including safeguards that regulate a government's access to personal data for national security and surveillance purposes.[17]

The justices at the CJEU seem determined to restrict cross-border transfers of personal data when necessary to protect the fundamental rights of natural persons. In the 2015 *Schrems* ruling, the CJEU struck down a significant legal basis for transferring personal data from the EU to the United States—the "Safe Harbor."[18] In two pending cases, parties have asked the CJEU again to interpret the legality of transfers of personal data to the United States, which, according to the submissions, presumably conducts mass surveillance.[19] The CJEU's rulings in these cases should afford greater clarity about the constitutional consequences for EU data protection law if a third country surveils commercial personal data flows from individuals in the EEA. Facing its own constitutional constraints and the commitments under the GATS, the EU may find itself between a rock and a hard place.

Human Rights, Compatibility with Internal EU Law, and Autonomy of the EU Legal Order

The EU, which has the exclusive competence over external trade policy and personal data protection, had to reconcile its position in digital trade diplomacy with internal EU law. There are two interrelated possible arguments for the supremacy under EU law of the protection of fundamental rights over international trade obligations: (1) the duty to ensure compatibility between EU law and international agreements; and (2) the principle of autonomy of the EU legal order vis-à-vis international law.

First, compatibility with internal EU policies is a key condition for the EU during its external negotiations. When negotiating international trade agreements, the competent EU institutions—the Council and the Commission—are "responsible for ensuring that the agreements negotiated are compatible with internal Union policies and rules."[20] Before an international agreement enters into force, a special legal procedure offers, as a second line

[14] Christopher Kuner, *Developing an Adequate Legal Framework for International Data Transfers*, *in* Reinventing Data Protection? 269–71 (Serge Gutwirth et al. eds., 2009).

[15] *See* Schrems, *supra* note 7, at para. 92; Opinion 1-15 on Draft EU-Canada PNR Agreement, ECLI:EU:C:2017:592, para. 140 (Eur. Ct. Justice, July 26, 2017) [hereinafter CJEU Opinion 1/15].

[16] EU Charter, *supra* note 2, art. 52(1); Schrems, *supra* note 7, at paras. 93–95; CJEU Opinion 1/15, *supra* note 15, at paras. 141, 154.

[17] GDPR, *supra* note 3, art. 45(2)(a).

[18] Schrems, *supra* note 7, at paras. 87–98.

[19] *See* Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems, Case C-311/18 (pending); La Quadrature du Net & Others v. Comm'n, Case T-738/16 (pending).

[20] Consolidated Version of the Treaty on the Functioning of the European Union art. 207(3)(2), 2010 O.J. (C 83) 47 (Mar. 30, 2010) [hereinafter TFEU].

https://doi.org/10.1017/aju.2019.81 Published online by Cambridge University Press

of defense for EU institutions and member states, an opportunity to request a CJEU opinion on the compatibility of the agreement with the EU's aquis. An example to that point is the opinion of the Court on the compatibility of the envisaged agreement between the EU and Canada on the transfer of Passenger Name Record data in the context of bilateral law enforcement cooperation. Here the justices concluded that several provisions of the envisaged agreement are not limited to what is strictly necessary and do not lay down clear and precise rules governing the transfer of personal data.[21] If the Court finds that the agreement is incompatible with the EU treaties, it cannot take effect unless amended or unless the treaties are revised.[22]

Second, the hierarchy of EU law and the principle of autonomy of the EU legal order vis-à-vis international law ensure the supremacy of the EU treaties over international agreements. International trade agreements concluded by the EU form an "integral part" of the EU legal system and are ranked below EU primary law, i.e., below the EU Charter and the founding treaties. According to the case law of the CJEU, which has declared itself the judicial guardian of the autonomy of the EU legal order, international agreements must respect the constitutional values and internal division of competences in the EU. However, as shown above, the CJEU will only deem an international agreement to be compatible with the EU Charter if it contains substantial constitutional safeguards on the protection of personal data.

The EU's Cross-Border Data Flows Proposal

The EU's negotiating position on cross-border data flows emerged in 2018 as a result of an interinstitutional dialogue that aimed to reconcile the EU's digital trade ambitions with its internal personal data protection framework. This happened against the backdrop of warnings, illuminated above, that the general exception for privacy and data protection in the GATS may be too narrow to justify restrictions on cross-border transfers of personal data under the GDPR.[23] The tension between EU data protection and trade law increased as the EU went into negotiations of trade commitments on unrestricted cross-border data flows in the new generation trade agreements.

To alleviate this tension, the EU's negotiating position carefully carves out the EU's own restrictions on cross-border transfers of personal data from the proposed prohibition on restriction of cross-border data flows. This carve-out primarily takes the form of a broad exception for domestic privacy and personal data protection rules, which not only allows WTO members to adopt and maintain data protection measures that the EU (or other actors) *deem appropriate*, but also explicitly states that any rules for cross-border transfers of personal data constitute a priori appropriate measures and recognizes that the protection of privacy and personal data is a fundamental right. The EU has also included identical provisions in its proposals for digital trade chapters in the ongoing trade negotiations with Australia, Chile, Indonesia, Tunisia, and New Zealand.

The wording of the proposed exception approximates that of the national security exception in the GATS.[24] This exception allows a WTO member to take any action in violation of its trade commitments *which it considers necessary* for the protection of its essential security interests. As the WTO Panel recently explained, in contrast to the objective "necessity test" in the general exception, the legal meaning of the clause "which it considers" allows a WTO Member *itself* to determine the "necessity" of these measures."[25] Drawing this parallel demonstrates that the

[21] *See* CJEU Opinion 1/15, *supra* note 15, at para. 154f.

[22] TFEU, *supra* note 20, art. 218 sec. 11.

[23] *See, e.g.*, Irion et al., *supra* note 10.

[24] General Agreement on Trade in Services art. XIVbis(1)(b), Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1B, 1869 UNTS 183.

[25] Panel Report, Russia-Measures Concerning Traffic in Transit, WT/DS512/R (adopted Apr. 26, 2019).

https://doi.org/10.1017/aju.2019.81 Published online by Cambridge University Press

EU's proposed exception for privacy and data protection safeguards broader regulatory autonomy than the GATS general exception, where "necessity" of the contested measure is evaluated by trade adjudicators.

Placing privacy and data protection on the same level of importance as national security, the EU's negotiation position is fundamentally different from that of the United States.[26] The U.S. model typically includes a broad requirement not to prohibit or restrict any commercial cross-border transfers of information, including personal information, and an exception closely resembling the general exception in the GATS.

Conclusion

Regulation of cross-border (personal) data flows through trade agreements inevitably brings the constitutional and moral values pursued by different societies to the table of trade negotiations. For the EU, the core values at stake are the fundamental rights to the protection of privacy and personal data. Safeguarding a broad autonomy to maintain its data protection rules, including limitations on cross-border transfers of personal data, in its international trade agreements has become essential for the EU to be able to respect its own constitutional boundaries. Some might argue that the design of the mechanism for cross-border transfers in the GDPR is overly formalistic and not always consistent.[27] However, the EU takes the view that it is for the EU, not trade adjudicators, to decide how to implement fundamental rights protections in EU law. The EU cannot and *should not* embark on any international trade commitments that are incompatible with its domestic legal framework.

As trade negotiations on cross-border data flows increasingly become multilateral, a clash between domestic values and the goal of digital trade liberalization is inevitable. In digital trade negotiations between the EU and the United States, for example, different normative frameworks for privacy and data protection have been the primary source of disagreement. These disagreements resulted in a tug of war between the two trading partners, each of which is trying to advance its own regulatory models for cross-border data flows.[28] This puts other countries, such as Canada, in a difficult position: On the one hand, Canada is a party to the U.S.-Mexico-Canada Agreement and must comply with a free cross-border data flow obligation; on the other hand, the EU has afforded Canada an adequacy decision under the EU data protection framework, which implies certain restrictions on onward transfers of Europeans' personal data outside Canada.

During the prospective e-commerce negotiations at the WTO, discussions will revolve not only around privacy and data protection. Other public interests, especially national security, industrial policy, and digital sovereignty will also enter the scene as China, Russia, and multiple developing countries negotiate on cross-border data flows. Each country will likely strike a different balance between digital trade liberalization and its other non-trade policy priorities, reflecting their own constitutional traditions, level of digital and economic development, and the desire to withstand digital colonialism. The EU and United States commitments to their own mutually inconsistent approaches to regulating cross-border data flows could prove counterproductive in this multilateral setting. Conversely, the ability to agree on a common position could allow the EU and the United States to counterbalance the negotiating power of less democratic states such as China.

[26] *See* Inu Manak, *U.S. WTO E-Commerce Proposal Reads Like USMCA*, Int'l Econ. L. & Pol'y Blog (May 8, 2019).

[27] *See, e.g.*, Christopher Kuner, *Reality and Illusion in EU Data Transfer Regulation Post Schrems*, 18 German L.J. 881 (2017).

[28] *See* Svetlana Yakovleva, *Privacy Protection(ism): The Latest Wave of Trade Constraints on Regulatory Autonomy*, U. Miami L. Rev. (forthcoming).

https://doi.org/10.1017/aju.2019.81 Published online by Cambridge University Press