Privacy and Data Protection in the EU- and US-Led Post-WTO Free Trade Agreements

Svetlana Yakovleva

Contents

1 Introduction

Regulating privacy and personal data protection has traditionally been a prerogative of domestic legal regimes. These areas were traditionally outside the scope of international trade law. Until very recently, free trade agreements (FTAs), starting from the Marrakesh Agreement on the Establishment of the World Trade Organization (WTO),[1] referred to privacy and personal data protection as public policy

The author would like to thank Rudolf Adlung, Christoph Kiener, Markus Krajewski, Joanna Pocztowska, Oliver Prausmueller, Martin Roy and Benjamin Zasche.

[1]Marrakesh Agreement on the Establishment of the World Trade Organization (WTO) (WTO Agreement).

S. Yakovleva (✉)
Institute for Information Law (IViR), University of Amsterdam, Amsterdam, The Netherlands

De Brauw Blackstone Westbroek, Amsterdam, The Netherlands
e-mail: Mail@svyakovleva.com

R. T. Hoffmann, M. Krajewski (eds.), *Coherence and Divergence in Services Trade Law*, European Yearbook of International Economic Law,
https://doi.org/10.1007/978-3-030-46955-9_5

objectives that can justify derogation from a party's (or member's) commitments in trade in services, financial or telecommunications sectors. The WTO Agreement mentions the protection of privacy and(or) personal data in the general exception of Article XIV(c)(ii) of the General Agreement on Trade in Services[2] (GATS), exceptions in the GATS Annex on Telecommunications[3] and in the Understanding on Financial Services.[4] The EU- and US-led FTAs concluded after the WTO Agreement (post-WTO FTAs) and before 2018 generally followed the same path with the only difference that privacy and data protection also appeared in some e-commerce chapters.

As (personal) data and its unrestricted flows became an important ingredient of cross-border digital trade, regulating such flows as well as the protection of the rights to privacy and personal data protection, which is often viewed as reason to restrict the flows of personal data, gradually became contentious and politically sensitive issues in domestic and international trade politics.[5]

The European Union (EU) was one of the first to regulate cross-border transfers of personal data in the 1995 Data Protection Directive.[6] The recently adopted General Data Protection Regulation (GDPR)[7] further developed this framework by making it more robust on the one hand, and flexible on the other. Limitations on cross-border transfers under EU law are grounded in the protection of the rights to privacy and personal data as binding fundamental rights under the EU Charter of Fundamental Rights.[8] The EU privacy and data protection framework, arguably one of the strictest in the world, is deeply rooted in a European cultural preference for strong privacy protection and is viewed as integral part and key instantiation of the protection of human dignity.[9]

In short, under the GDPR, personal data can flow as freely as within the European Economic Area (EEA) to third countries that obtained a so-called adequacy decision from the European Commission, stating that they ensure an adequate level of

[2]General Agreement on Trade in Services, Annex 1B to the WTO Agreement.

[3]Article 5(d) GATS Annex on Telecommunication.

[4]Article B.8 of the 1994 Understanding on Commitments in Financial Services (Understanding).

[5]Wolfe (2019), p. s64.

[6]Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data OJ 1995 L 281, 31.

[7]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, OJ 2016 L 119/1-88.

[8]Charter of Fundamental Rights of the European Union, OJ 2012 C 326.

[9]Article 1 of the EU Charter; Explanation on Article 1—Human dignity in Explanations Relating to the Charter of Fundamental Rights, OJ 2007 C 303/17, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:303:0017:0035:en:PDF; Opinion of the European Data Protection Supervisor (EDPS) 4/2015 Towards a New Digital Ethics Data, Dignity And Technology, p. 12, 11 September 2015; Rodota (2009), p. 80.

personal data protection (currently 13 countries,[10] including the EU-US Privacy Shield framework,[11] and the mutual adequacy arrangement with Japan[12]). Transfers of personal data to other countries are only allowed if the data exporter has implemented adequate safeguards, such as the standard contractual clauses (SCCs) approved by the European Commission, binding corporate rules for multinational companies or companies conducting joint economic activity, approved industry codes of conduct or certification.[13] If it is not reasonably possible for a data exporter to adopt any of the above-mentioned safeguards, it may rely on specific derogations of Article 49 GDPR, which include explicit consent of an individual, necessity of transfer for the conclusion or performance of a contract, or necessity for the establishment, exercise or defence of legal claims. The EU's "border control" approach to cross-border transfers of personal data has always been in sharp contrast with the US "open skies" policy in this domain.[14] Several scholars warned that it may even run afoul of the EU's WTO trade in services commitments.[15]

Shortly after the conclusion of the WTO agreement, negotiated before the proliferation of Internet, WTO members realised the importance of e-commerce for international trade. As the WTO Work Programme on E-Commerce, launched in 1998,[16] was not yielding any meaningful results, the negotiations on this issue have shifted to bi-lateral and regional fora. Starting from early 2000s, non-binding provisions on electronic commerce appeared in FTAs, which also often mentioned the protection of privacy and personal data.[17] With these provisions trading partners embarked on a learning curve that paved the way for the "next generation" of binding electronic commerce (or digital trade) provisions.[18]

In the spirit of its "digital trade" agenda, the United States has been a pioneer in including provisions on free cross-border data flows in international trade

[10]European Commission, Adequacy of the protection of personal data in non-EU countries https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en.

[11]Commission Implementing Decision (EU) 2016/1250 of 12 July 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, OJ 2016 L207/1.

[12]European Commission, European Commission adopts adequacy decision on Japan, creating the world's largest area of safe data flows, 23 January 2019 http://europa.eu/rapid/press-release_IP-19-421_en.htm.

[13]Articles 40(2), 42(2), 46 GDPR.

[14]Svantesson (2011), p. 184; LeSieur (2012), pp. 101, 103, 104.

[15]Swire and Litan (1998), pp. 188–196. On the contrary, Shaffer argued that a hypothetical US claim regarding WTO inconsistency of EU's framework for personal data transfers "would likely not prevail." Shaffer (2000), pp. 46–51.

[16]WTO, Work programme on electronic commerce, WT/L/274, 30 September 1998.

[17]Burri (2017b), pp. 18 and 22.

[18]Wolfe (2019), p. s78.

agreements.[19] The United States first proposed a *binding* horizontal provision on free cross-border data flows in the drafts of the currently stalled Trans-Atlantic Trade and Investment Partnership (TTIP) and Trade in Services Agreement (TiSA).[20] This attempt later, as discussed in Sect. 5.2 below, proved successful in the negotiations of the Comprehensive and Progressive Trans-Pacific Partnership (CPTPP),[21] drafted before the US withdrawal from the Agreement,[22] the United States – Mexico – Canada Agreement (USMCA),[23] and the U.S. – Japan Digital Trade Agreement.[24] The e-commerce chapter of the CPTPP, and the digital trade chapter of the USMCA and the U.S. – Japan Digital Trade Agreement not only include a legally binding horizontal obligation on cross-border data flows, but also extensive provisions on the protection of privacy and personal information[25] (I will refer to these provisions jointly as "digital trade provisions"). In 2018, the European Commission reached a political agreement on the EU position on the model provisions for EU-led trade agreements on cross-border data flows. While tackling the same issues, the EU model provisions reserve a wide policy space for the protection of privacy and personal data as fundamental rights. These developments unfolded against the backdrop of an emerging patchwork of domestic rules hampering cross-border data flows, such as those adopted by Russia and China and are underway in India, Indonesia, Malaysia, Singapore and Chile.[26] The new digital trade provisions not only set boundaries on domestic restrictions on cross-border data flows, but also create a basis for regulatory cooperation.[27] On January 25, 2019, 76 members of the World Trade Organization (WTO) launched talks on electronic commerce, which,

[19]Burri (2017a), p. 99; Aaronson (2016), p. 59; Geist M (2018) Data rules in modern trade agreements: toward reconciling an open internet with privacy and security safeguards. CIGI International Policy Considerations, https://www.cigionline.org/articles/data-rules-modern-trade-agreements-toward-reconciling-open-internet-privacy-and-security.

[20]Le Roux (2017); Fontanella-Khan J., Data Protection Ruled out of EU-US Trade Talks, Financial Times, 4 November 2013.

[21]Comprehensive and Progressive Agreement for Trans-Pacific Partnership, 8 March, 2018, https://www.mfat.govt.nz/assets/Trans-Pacific-Partnership/Text/14.-Electronic-Commerce-Chapter.pdf.

[22]Letter from the Executive Office of the President, Office of the United States Trade Representative, 30 January 2017, https://ustr.gov/sites/default/files/files/Press/Releases/1-30-17%20USTR%20Letter%20to%20TPP%20Depositary.pdf.

[23]Agreement between the United States of America, the United Mexican States, and Canada (USMCA), signed 30 November 2018, https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/agreement-between.

[24]United States – Japan Digital Trade Agreement, signed on 7 October 2019, https://ustr.gov/sites/default/files/files/agreements/japan/Agreement_between_the_United_States_and_Japan_concerning_Digital_Trade.pdf.

[25]"Personal information" is a U.S. law term for "personal data."

[26]Geist M (2018) Data rules in modern trade agreements: toward reconciling an open internet with privacy and security safeguards. CIGI International Policy Considerations, https://www.cigionline.org/articles/data-rules-modern-trade-agreements-toward-reconciling-open-internet-privacy-and-security.

[27]Wolfe (2019), pp. s65–s66.

among other things will cover rules on cross-border data flows and the protection of the rights to privacy and personal data.[28]

This chapter takes stock of the evolution of provisions on privacy and data protection in the post-WTO FTAs and FTAs currently under negotiation. It evaluates the trends and patterns of the development of these provisions and provides an outlook for the upcoming negotiations on electronic commerce at the WTO.

The analysis in this chapter relies on the EU-led FTAs concluded after 2000, which include provisions on e-commerce: the 2000 EU–Mexico economic partnership agreement[29] complemented by the 2001 EU–Mexico Joint Council Decision implementing this agreement[30] (collectively referred to as "EU-Mexico EPA"); the 2003 EU–Chile association agreement;[31] the 2012 EU–Central America association agreement;[32] the 2011 EU–Korea FTA;[33] the 2012 trade agreement between the EU, Colombia, and Peru;[34] the 2014 EU–Singapore FTA;[35] the 2016 EU–Canada Comprehensive Economic and Trade Agreement (CETA),[36] EU-Japan Economic

[28]European Commission, 76 WTO Partners Launch Talks on E-commerce, 25 January 2019, http://trade.ec.europa.eu/doclib/press/index.cfm?id=1974&title=76-WTO-members-launch-talks-on-e-commerce; Foroohar R., Nations Move to Avoid Global Ecommerce 'Splinternet', Financial Times, 24 January 2019.

[29]Economic Partnership, Political Coordination and Cooperation Agreement between the European Community and its Member States, of the One Part, and the United Mexican States, of the Other Part, 8 December 1997 OJ 2000 L 276/45, https://eeas.europa.eu/sites/eeas/files/28.10.2000_mexico.pdf.

[30]Decision No. 2/2001 of the EU–Mexico Joint Council of 27 February 2001 implementing Articles 6, 9, 12(2)(b), and 50 of the Economic Partnership, Political Coordination and Cooperation Agreement (2001/153/EC) OJ 2001 L70, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2001.070.01.0007.01.ENG.

[31]Agreement Establishing an Association between the European Community and Its Member States, of the One Part, and the Republic of Chile, of the Other Part, 11 November 2002 OJ 2002 L 352/3, http://eur-lex.europa.eu/resource.html?uri=cellar:f83a503c-fa20-4b3a-9535-f1074175eaf0.0004.02/DOC_2&format=PDF.

[32]Agreement Establishing an Association between Central America, on the one hand, and the European Union and its Member States, on the other, 29 June 2012 OJ 2012 L 346/3, http://eur-lex.europa.eu/legal-content/en/TXT/PDF/?uri=CELEX:22012A1215(01)&rid=1.

[33]Free Trade Agreement Between the European Union and its Member States, of the One Part, and the Republic of Korea, of the Other Part, 6 October 2010 OJ 2011 L. 127/6, http://eur-lex.europa.eu/legal-content/en/TXT/PDF/?uri=CELEX:22011A0514%2801%29&rid=1.

[34]Trade Agreement Between the European Union and its Member States, of the One Part, and Colombia and Peru, of the Other Part, 31 May 2012 OJ 2012 L 354/1, http://publications.europa.eu/resource/cellar/e4c7ab87-4a17-11e2-8762-01aa75ed71a1.0001.04/DOC_30.

[35]EU-Singapore Free Trade Agreement (not yet ratified by the EU). Text available at https://trade.ec.europa.eu/doclib/press/index.cfm?id=961.

[36]Comprehensive Economic and Trade Agreement (CETA) between Canada, of the one part, and the European Union and its Member States, of the other part, 14 September 2014 OJ 2017 L 11/23, http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:22017A0114(01)&from=EN.

Partnership Agreement (JEFTA)[37] and draft EU-Mexico FTA (revision of EU-Mexico EPA).[38] The analysis also considers the EU proposals for the electronic commerce negotiations at the WTO,[39] FTAs with Australia,[40] Chile,[41] Indonesia,[42] New Zealand[43] and Tunisia.[44] Among the US-led FTAs the chapter analyses the FTAs concluded after the so-called US "Digital Agenda,"[45] namely FTAs with Australia,[46] Bahrain,[47] the Central American countries,[48] Chile,[49] Morocco,[50]

[37]EU-Japan Economic Partnership Agreement (JEFTA), text after legal revision available at https://trade.ec.europa.eu/doclib/press/index.cfm?id=1684.

[38]European Commission, New EU-Mexico agreement: The Agreement in Principle and its texts, http://trade.ec.europa.eu/doclib/press/index.cfm?id=1833.

[39]European Commission, EU Proposal for WTO Disciplines and Commitments Relating to Electronic Commerce, INF/ECOM/22, 2.7–2.8, 26 April 2019, http://trade.ec.europa.eu/doclib/docs/2019/may/tradoc_157880.pdf.

[40]EU Proposal for the Digital Trade Chapter of EU-Australia *FTA* (Oct. 10, 2018), http://trade.ec.europa.eu/doclib/docs/2018/december/tradoc_157570.pdf.

[41]On file with Author. EU's proposal for Digital Trade chapter of a possible modernised EU-Chile Association Agreement is not yet publicly available.

[42]European Commission, Report of the 5th Round of Negotiations for a Free Trade Agreement Between the European Union and Indonesia, 9–13 July 2018, http://trade.ec.europa.eu/doclib/docs/2018/july/tradoc_157137.pdf.

[43]EU Proposal for the Digital Trade Chapter of EU-New Zealand *FTA*, 25 September 2018, http://trade.ec.europa.eu/doclib/docs/2018/december/tradoc_157581.pdf.

[44]On file with Author. EU's proposal for Digital Trade chapter of a possible modernised EU-Tunisia FTA is not yet publicly available.

[45]Bipartisan Trade Promotion Authority Act of 2002, sections 2102(b)(8) and 2102(b)(9). Wunsch-Vincent (2003), p. 7.

[46]United States-Australia Free Trade Agreement, with Annexes and Related Exchange of Letters, 18 May 2004, 43 I.L.M. 1248, https://ustr.gov/trade-agreements/free-trade-agreements/australian-fta/final-text.

[47]United States-Bahrain Free Trade Agreement, 14 September 2004, 44 I.L.M. 544, https://ustr.gov/trade-agreements/free-trade-agreements/bahrain-fta/final-text.

[48]Dominican Republic-Central America-United States Free Trade Agreement, 28 May 2004, 43 I.L.M. 514, https://ustr.gov/trade-agreements/free-trade-agreements/cafta-dr-dominican-republic-central-america-fta/final-text.

[49]United States-Chile Free Trade Agreement Implementation Act, Pub. L. No. 108-77 (2003) https://ustr.gov/trade-agreements/free-trade-agreements/chile-fta/final-text.

[50]United States-Morocco Free Trade Agreement, 15 June 2004, 44 I.L.M. 544, https://ustr.gov/trade-agreements/free-trade-agreements/morocco-fta/final-text.

South Korea (KORUS),[51] Oman,[52] Panama,[53] Peru,[54] Singapore,[55] Colombia,[56] and the most recent USMCA and U.S. – Japan Digital Trade Agreement. The analysis also includes CPTPP (to which the US is not a party) because the relevant digital trade provisions were not altered after the US withdrawal from the agreement. They also formed the basis for the US model approach implemented in the USMCA and other smaller FTAs.[57]

The chapter proceeds as follows. Sections 2–5 map out, respectively, the evolution of provisions on privacy and personal data protection in general exceptions, financial and telecommunications chapters, chapters on electronic commerce and digital trade. Each section identifies trends in the design and wording of these provisions in the EU- and US-led FTAs and explicates the points of convergence and divergence between the EU and US approaches. Section 6 concludes.

2 General Exception for Privacy and Data Protection

The GATS general exception explicitly mentions privacy and personal data protection as legitimate policy objectives that could justify a violation of a WTO member's commitments under the GATS. Article XIV(c)(ii) reads as follows:

> Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services, nothing in this Agreement shall be construed to prevent the adoption or enforcement by any Member of measures . . .
>
> (c) *necessary* to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to . . .

[51] United States-Korea Free Trade Agreement, 1 April 2007, 46 I.L.M. 642 https://ustr.gov/trade-agreements/free-trade-agreements/korus-fta/final-text.

[52] United States-Oman Free Trade Agreement, 1 January 2006, https://ustr.gov/trade-agreements/free-trade-agreements/oman-fta/final-text.

[53] United States-Panama Trade Promotion Agreement, 31 October 2012, https://ustr.gov/trade-agreements/free-trade-agreements/panama-tpa/final-text.

[54] United States-Peru-Trade Promotion Agreement, 12 April 2006, https://ustr.gov/trade-agreements/free-trade-agreements/peru-tpa/final-text.

[55] United States-Singapore Free Trade Agreement, 3 September 2003, 117 Stat. 948 https://ustr.gov/trade-agreements/free-trade-agreements/singapore-fta/final-text.

[56] United States-Colombia Trade Promotion Agreement, 15 May 2012, https://ustr.gov/trade-agreements/free-trade-agreements/colombia-fta/final-text.

[57] Geist M (2018) Data rules in modern trade agreements: toward reconciling an open internet with privacy and security safeguards. CIGI International Policy Considerations, https://www.cigionline.org/articles/data-rules-modern-trade-agreements-toward-reconciling-open-internet-privacy-and-security; Burri (2017a), p. 101.

(ii) the *protection of the privacy of individuals in relation to the processing and dissemination of personal data* and the protection of confidentiality of individual records and accounts <. . .> (emphasis added)

One of the core elements of the general exception is the "necessity test." Although the application of this test has been uneven in the past, it could be argued that, in most cases, "necessity" boils down to an assessment of whether a less trade restrictive measure is "reasonably available" to a defending party.[58] This test has been criticized for being insufficiently broad to justify domestic fundamental rights-based restrictions on cross-border data flows, such as those adopted by the EU, should they be challenged under the GATS most-favored nation treatment or national treatment provisions.[59]

In all the EU and US-led post-WTO FTAs considered in this article the wording of the general exception for domestic privacy and data protection legal frameworks has been either modelled after the above-mentioned general exception of the GATS or incorporated this exception *mutatis mutandis*.[60] This, however, does not mean that the EU and US agree on the breadth of the regulatory space that FTAs should grant domestic privacy and data protection regulation. On the contrary, in the context of digital trade negotiations, as Sect. 5 explicates, this has become one of the most controversial issues on which the EU and US positions are widely divergent.

3 Telecommunications and Financial Services Chapters

Starting from the WTO Agreement, financial and telecommunications services chapters mention the protection of confidentiality of messages, privacy or personal data as an exception or a counterbalancing provision to the obligation to provide access to public telecommunications infrastructure and to allow free cross-border flows of financial data.

Under article 5(d) of the GATS Annex on Telecommunication, a member may derogate from an obligation to provide access to public telecommunications infrastructure if this is "*necessary* to ensure the *security and confidentiality of messages*, subject to the requirement that such measures are *not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised*

[58] Regan (2007), p. 350; Venzke (2011), p. 1138.

[59] Yakovleva (2018), pp. 497–499.

[60] See e.g. Article 28.3(2)(c)(ii) CETA, Article 8.62(e)(ii) EU-Singapore FTA, Article 167(1)(e)(ii) FTA between EU, Colombia and Peru, Article 27(2) EU-Mexico Joint Council Decision, Article 7.50(e)(ii) EU-Korea FTA, Article 203(1)(e)(ii) EU Association Agreement with Central America, Article 135(1)(e)(ii) EU-Chile Association Agreement, Article 22.1(2) US-Australia FTA, Article 23.1(2) KORUS FTA, Article 21.1(2) US-Singapore FTA, Article 21.1(2) Dominican Republic-Central America-United States FTA, Article 21.1(2) US – Panama PTA, Article 32.1(2) USMCA, Article 29.1(3) CPTPP.

restriction on trade in services." The wording of this exception closely resembles the structure and wording of the general exception discussed in the previous section.

While the GATS Annex on Telecommunications does not specifically mention privacy, CETA and some of the US-led FTAs refer to privacy in addition to the security and confidentiality of the communications.[61] EU-led FTAs before and after CETA follow the GATS Annex on Telecommunications model in this respect.[62] Until very recently, all EU-led FTAs considered in this article no longer formulated this provision as an exception, but as a positive obligation of the parties to take appropriate measures to protect privacy of electronic communications ("a Party shall").[63] Furthermore, these provisions contained a lower threshold, as compared with the GATS Annex on Telecommunications, that the measures to protect privacy and/or confidentiality of electronic communications should meet ("necessity" of such measures was not required).[64] This trend has reversed in the most recent EU-led FTA – JEFTA—and the draft EU-Mexico FTA, which almost verbatim repeat the GATS model.[65] While the EU approach to formulating privacy-related provisions has varied, post-WTO US-led FTAs consistently follow the model of the exception from the GATS Annex on Telecommunications.[66]

In the WTO Agreement, a privacy and data protection-related provision in financial services sector is included in Article B.8 of the 1994 Understanding on commitments in financial services (Understanding) to counterbalance the provision on the free flow of financial information. The provision reads as follows:

> . . . Nothing in this paragraph restricts the right of a Member to protect *personal data, personal privacy* and the confidentiality of individual records and accounts so long as such right is *not used to circumvent* the provisions of the Agreement. (emphasis added)

As compared to the general exception for privacy and data protection, this sectoral exception does not provide for a "necessity" requirement.

---

[61] Article 15.3(4) of CETA, article 9.2(4) of US – Singapore FTA, article 13.2(4) of Dominican Republic-Central America-United States FTA, article 13.2(4) of the US – Panama TPA, article 13.2 (4) of US-Chile FTA, article 13.2(4) of US-Morocco FTA, article 14.2(4) of US-Peru FTA, article 14.2(4) of US-Colombia FTA, article 18.3(4) of USMCA, article of 13.4(4) CPTPP.

[62] Article 8.27 of EU-Singapore FTA, article 149 of FTA between EU, Colombia and Peru, article 7.35 of EU-Korea FTA, article 192 of the EU association agreement with Central America, article 8.44(4) of JEFTA, article TS.6(4) of draft Telecommunications chapter of modernised EU-Mexico FTA.

[63] For discussion see Yakovleva (2018), pp. 492–294.

[64] See e.g. article 15.3(4) of CETA.

[65] Article 8.44(4) of JEFTA, article TS.6(4) of draft Telecommunications chapter of modernised EU-Mexico FTA.

[66] Article 9.2(4) of US – Singapore FTA, article 13.2(4) of Dominican Republic-Central America-United States FTA, article 13.2(4) of US – Panama TPA, article 13.2(4) of US-Chile FTA, article 13.2(4) of US-Morocco FTA, article 14.2(4) of US-Peru FTA, article 14.2(4) of US-Colombia FTA, article 12.2(4) of US – Australia FTA, article 14.2(4) of KORUS FTA, article 12.2(4) US-Bahrain FTA, article 13.2(4) of US-Oman FTA, article 18.3(4) USMCA, article 13.4(4) CPTPP.

Provisions on privacy and data protection in financial services chapters of EU-led post-WTO FTAs exhibit a similar dynamic as in that in telecommunications chapters. While the wording of obligations on free flow of financial information remained constant,[67] until very recently all post-WTO EU-led FTAs formulated the provision on the protection of privacy and personal data as a positive obligation ("[e]ach Party shall maintain adequate safeguards to protect privacy").[68] Furthermore, as compared with that of Understanding, these provisions do not contain an anti-circumvention requirement; instead they state that measures protecting privacy and personal data be "appropriate" or "adequate."[69] In JEFTA, however, the EU has returned to the model of the Understanding.[70] The financial services chapter of the draft EU-Mexico FTA does not contain provisions on cross-border data flows of financial data and the protection of privacy and personal data; it merely includes a three years' review clause allowing the parties to reassess whether such provisions are necessary.[71]

Research into the US-led post-WTO FTAs reveals a remarkably different approach to cross-border data flows and privacy and data protection in financial services. Only KORUS and USMCA include provisions on cross-border flows of financial data.[72] In CPTPP financial data flows are regulated by a horizontal provision on data flows discussed in Sect. 5 below. While financial services chapter of KORUS does not contain a specific exception or counterbalancing provision on data protection, this exception in CPTPP and USMCA follow the model of Understanding. The exception for privacy and data protection in these FTAs is broader than the exception from a horizontal provision on cross-border data flows discussed in Sect. 5 below because it does not require that measures to protect privacy and personal data should be "necessary."

To conclude, in the last two decades the US approach to including and formulating provisions on privacy and data protection into telecommunications and financial services chapters has been more internally consistent and more coherent with the WTO Agreement, than that of the EU. Until a recent return to the WTO model in JEFTA and the draft EU-Mexico FTA, the EU tended to afford more policy space to domestic privacy and data protection rules vis-à-vis its international trade

[67] Article B.8 of Understanding on commitments in financial services, article 13.15(1) of CETA, article 157(1) of FTA between EU, Colombia and Peru, article 22(1) of the EU association agreement with Mexico, article 7.43(a) of EU-Korea FTA, article 198(1) of FTA between the EU and Central America, article 122(1) of the EU-Chile association agreement, article 8.54(1) of EU-Singapore FTA.

[68] Article 8.54(2) of EU-Singapore FTA, article 157(2) of FTA between EU, Colombia and Peru, article 198(2) of the EU association agreement with Central America, article 7.43(b) of EU-Korea FTA, article 22(2) of EU-Mexico Joint Council Decision, Article 13.15(2) of CETA.

[69] See e.g. article 8.54(2) of EU-Singapore FTA, article 157(2) of FTA between EU, Colombia and Peru, article 198(2) of the EU association agreement with Central America, article 7.43(b) of EU-Korea FTA, article 22(2) of EU-Mexico Joint Council Decision.

[70] Article 8.63(2) of JEFTA.

[71] Article XX.10 Chapter 12 of draft EU-Mexico FTA.

[72] Annex 13-B, section B of KORUS FTA, article 17.17 of USMCA.

obligations to provide access to public telecommunications infrastructure and to allow free cross-border flows of financial data than the WTO Agreement.

4 E-commerce Chapters

Before I delve into the privacy and data protection provisions in the e-commerce and digital trade chapters, an important clarification is in order. I make a distinction between e-commerce and digital trade solely for the purposes of this chapter to underscore a qualitative shift in regulating privacy and data protection in the FTAs concluded in 2018 or later, which make a special emphasis on digital trade. These include the US-led CPTPP, USMCA and the U.S. – Japan Digital Trade Agreement, EU-led JEFTA and the EU's negotiation position on cross-border data flows, which has not yet been included in any concluded FTA. The discussion on the difference between e-commerce and digital trade is beyond the scope of this chapter.

Unlike the WTO agreement, most EU- and US-led post-WTO FTAs contain a chapter on e-commerce.[73] However, while all e-commerce chapters in EU-led FTAs considered in this chapter mention privacy and data protection (some more extensively than others), this is the case in only a few of their US counterparts.

The e-commerce chapters in EU-led FTAs refer to privacy and data protection in three respects: in the chapter on the objectives of electronic commerce, as an alone-standing non-aspirational commitment to protect personal data and in the context of regulatory cooperation. None of these provisions are legally binding.[74] While the wording of each type of provision throughout different FTAs is fairly consistent, the combination of these provision from one FTA to another is heterogeneous.[75]

An example of the first type of provision is Article 8.57(4) "Objectives [of electronic commerce]" of the FTA with Singapore:[76]

> The Parties agree that the development of electronic commerce *must* be fully compatible with *international standards of data protection*, in order to ensure the confidence of users of electronic commerce. (italics added)

[73]Chapter 16 of CETA, chapter 8 Section F of EU-Singapore FTA, chapter 6 of FTA between EU, Colombia and Peru, chapter 7 section F of EU-Korea FTA, chapter 6 of the EU association agreement with Central America, chapter 16 of US-Australia FTA, chapter 15 of KORUS FTA, chapter 14 of US-Singapore FTA, chapter 14 of US-Central America FTA, chapter 14 of US-Panama FTA, chapter 13 of US-Bahrain FTA, chapter 15 of US-Chile FTA, chapter 14 of US-Morocco FTA, chapter 14 of US-Oman FTA, chapter 15 of US-Peru FTA, chapter 15 of US-Colombia PTA.

[74]Yakovleva (2018), p. 496.

[75]See also Monteiro and Teh (2017), p. 71.

[76]See also article 162(2) of FTA between EU, Colombia and Peru, article 7.48(2) of EU-Korea FTA, article 201(2) of the EU association agreement with Central America.

The reference to international standards on data protection is of marginal relevance, as these standards are highly fragmented.[77]

An example of the second type of provision is Article 164 of the FTA with Colombia and Peru, which requires that parties "shall endeavour, insofar as possible, and within their respective competences, to develop or maintain, as the case may be, regulations for the protection of personal data".[78]

The third type of provision typically requires that the parties maintain a dialogue on regulatory issues relating to, raised by or relevant for the development of electronic commerce.[79] As a rule, this provision contains an open list of relevant issues, which sometimes explicitly mentions the protection of personal data (or personal information).

Of all e-commerce chapters in US-led FTAs concluded before 2018 and considered in this chapter, only three mention the protection of privacy or personal information.

Article 15.8 of KORUS FTA includes a non-binding provision on cross-border information flows—the first of its kind—which in passing also refers to the protection of personal information:

> Recognizing the importance of the free flow of information in facilitating trade, and *acknowledging the importance of protecting personal information*, the Parties *shall endeavor to refrain* from imposing or maintaining unnecessary barriers to electronic information flows across borders.

The US-Panama PTA and the US-Chile FTA mention the protection of privacy in the context of regulatory cooperation on e-commerce.[80]

To conclude, the EU has been more proactive than the US in including privacy and data protection-related provisions in e-commerce chapters. Although all those provisions are purely aspirational, their consistent presence in e-commerce chapters asserts the particular importance of privacy and personal data protection as (at times) competing public policy objectives in regulation of e-commerce by international trade.

5 Regulating Privacy and Data Protection in Digital Trade Chapters

Both the EU and the US are actively negotiating digital trade provisions, which include clauses on the protection of privacy and personal data. These provisions take the form of exceptions from horizontal obligations on cross-border data flows and

[77] For a discussion see Yakovleva (2018), pp. 482–487 and 498.

[78] Article 164 of FTA between EU, Colombia and Peru.

[79] Article 202 of the EU Association agreement with Central America, article 7.49(1) of EU-Korea FTA, article 16.6(1) of CETA, article163(1) of FTA between EU, Colombia and Peru.

[80] Article 14.5 of US-Panama TPA, article 15.5 of US-Chile FTA.

extensive clauses on the protection of privacy and personal data (information). Although both the EU and the US aim at achieving the same goal—curtailing "digital protectionism"—their understanding of what it entails and the appetite for domestic regulatory autonomy to protect privacy and personal data are sharply contrasting.[81] While the US often labels onerous data protection rules as "digital protectionism," the EU excludes from "digital protectionism" measures that "can be justified with legitimate privacy considerations."[82] This section explicates the differences in the EU and US approaches.

5.1 *The EU Approach to Privacy and Data Protection in Digital Trade Chapters*

Most of the discussions on privacy and personal data protection in the context of digital trade revolve around horizontal obligations prohibiting restrictions of cross-border data flows. The source of the controversy is that these provisions could be in direct conflict with the EU's restrictions on cross-border transfers of personal data under the GDPR. Therefore, the EU can undertake this obligation, while ensuring internal consistency of its *aquis*, only under the condition that an exception from such an obligation is sufficiently broad to accommodate the EU's limitations on personal data transfers.[83] Overall, the EU has been cautious in including commitments on cross-border data flows in its FTAs.[84]

The possibility of inclusion of a binding cross-border data flow provision accompanied by a GATS Article XIV(c)(ii)-type exception for data protection in the Trade in Services Agreement (TiSA) and the Transatlantic Trade and Investment Partnership (TTIP)—both now stalled—sparked a strong push back from academics and civil society in 2015–2016.[85] The main point of concern was that the exception was too narrow and the EU's framework for personal data transfers may not be able to

[81]For discussion, see Yakovleva (2020).

[82]Compare Aaronson (2017), pp. 8–10 with Communication from the European Commission, *Exchanging and Protecting Personal Data in a Globalised World*, 10 January 2017, p. 6 (Jan. 10, 2017), https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017DC0007&from=EN. See also Yakovleva (2020).

[83]Yakovleva and Irion (2020).

[84]Burri (2017b), p. 22.

[85]See Irion et al. (2016), pp. 44–45 and 59–60, Fernández Pérez M., Corporate-sponsored privacy confusion in the EU on trade and data protection, EDRI, 12 October 2016, https://edri.org/corporate-sponsored-privacy-confusion-eu-trade-data-protection/, European Parliament resolution of 8 July 2015 containing the European Parliament's recommendations to the European Commission on the negotiations for the Transatlantic Trade and Investment Partnership (TTIP) (2014/2228 (INI)), European Parliament resolution of 3 February 2016 containing the European Parliament's recommendations to the Commission on the negotiations for the Trade in Services Agreement (TiSA) (2015/2233(INI)).

pass its threshold. This opposition lead to an interinstitutional dialogue within the European Commission. In the meantime, the EU refrained from including any provision on cross-border data flows in the JEFTA and the draft EU-Mexico FTA. In both cases this provision was replaced by a review clause, allowing the parties to revisit the issue in three years' time.[86] In the case of Japan, the absence of such clause was ameliorated by the adoption of a mutual adequacy decision under the GDPR shortly before JEFTA took effect. In addition, JEFTA's Regulatory Cooperation chapter contains an additional safeguard for the Parties' level of privacy and data protection. Articles 18.1(2)(h) and 18.1(3) allow each Party, notwithstanding regulatory cooperation measures, to "to define or regulate its own levels of protection in pursuit or furtherance of its public policy objectives in areas such as personal data and cybersecurity" and to adopt, maintain and apply regulatory measures "in accordance with its legal framework, principles and deadlines, in order to achieve its public policy objectives at the level of protection it deems appropriate."

In 2018 the European Commission reached a political agreement on the EU position on cross-border data flows. This position was expressed in the model clauses, which consist of a model provision on cross-border data flows (Article A), an exception for the protection of privacy and personal data (Article B), and a provision excluding the parties' rules and safeguards for the protection of personal data and privacy, including cross-border data transfers of personal data, from the scope of regulatory cooperation (Article X).[87] For the purposes of this chapter, I will only consider model Articles A and B.

The EU has already included the model provisions in its negotiating proposals for digital trade chapters in the currently negotiated trade agreements with New Zealand, Australia, Indonesia, Chile and Tunisia.[88] The same model clauses are incorporated into the recent EU proposal for WTO rules on electronic commerce.[89]

---

[86]Article 8.81 of JEFTA, article XX Chapter 16 of draft EU-Mexico Free Trade Agreement, Fortnam (2017).

[87]Horizontal provisions for cross-border data flows and for personal data protection (in EU trade and investment agreements) http://trade.ec.europa.eu/doclib/docs/2018/may/tradoc_156884.pdf.

[88]EU's proposal for the Digital Trade Chapter of EU-New Zealand FTA, 25 September 2018, http://trade.ec.europa.eu/doclib/docs/2018/december/tradoc_157581.pdf, EU's proposal for the Digital Trade chapter of EU-Australia FTA, 10 October 2018, http://trade.ec.europa.eu/doclib/docs/2018/december/tradoc_157570.pdf, European Commission, Report of the 5th round of negotiations for a Free Trade Agreement between the European Union and Indonesia, 9 to 13 July 2018 http://trade.ec.europa.eu/doclib/docs/2018/july/tradoc_157137.pdf, EU's proposal for a Digital Trade chapter for a Deep and Comprehensive Free Trade Area (DCFTA) with Tunisia, 9 November 2018, https://trade.ec.europa.eu/doclib/docs/2019/january/tradoc_157660.%20ALECA%202019%20-%20texte%20commerce%20numerique.pdf, the available EU's proposal for Digital Trade chapter of a possible modernised EU-Chile Association Agreement of 5 February 2018 only contains a placeholder for provisions on data flows, https://trade.ec.europa.eu/doclib/docs/2018/february/tradoc_156582.pdf.

[89]Communication from the European Union, EU proposal for WTO disciplines and commitments relating to electronic commerce, INF/ECOM/22, 26 April 2019, http://trade.ec.europa.eu/doclib/docs/2019/may/tradoc_157880.pdf.

Article A prohibits four types of restrictions of cross-border data flows: (1) a requirement to use local computing facilities or network elements; (2) a requirement to localize data on a Party's territory for storage or processing; (3) the prohibition to store or process data in the territory of the other Party; and (4) the prohibition of making the cross-border transfer of data contingent upon use of computing facilities or network elements in the Parties' territory or upon localisation requirements in the Parties' territory. None of these prohibitions capture the EU's own restrictions on cross-border transfers of personal data.

Article B declares the protection of personal data and privacy as a fundamental right, which reflects the EU's own approach to the protection of these policy interests. In addition, it contains a broad national security-type exception for domestic privacy and data protection regime, which allows each party to 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*' (emphasis added).

In the existing body of international trade law, a similar formula was used for a national security exception in Article XXI of the General Agreement on Tariffs and Trade of 1947 (GATT 1947), which was later incorporated into GATT 1994, and Article XIVbis(1)(b) of the GATS, which states:

> Nothing in this Agreement shall be construed:
>
> (b) to prevent any Member from taking any action which *it considers necessary for* the protection of its essential security interests <. . .> .[90] (emphasis added)

The scarce practice of the GATT/WTO Council relating to the national security exception,[91] and the recent WTO Panel decision in *Russia – Traffic in Transit*[92] show that although the exception is not totally "self-judging" and the WTO adjudicating bodies have a power to review that that the objective requirements of the exception are met,[93] the WTO member invoking the exception has a wide margin of appreciation.[94] It is up to this member to decide *whether* an action is required, and *which* action should be taken; this choice cannot be questioned by a trade adjudicating body.[95] In *Russia – Traffic in Transit*, the WTO Panel explicitly stated that the

[90]The same provision is also envisaged in Article 73 of the Agreement on Trade Related Aspects of Intellectual Property Rights (TRIPS), and several international trade agreements adopted after the Uruguay Round.

[91]Cottier and Delimatsis (2008), pp. 329–348.

[92]*Russia — Measures Concerning Traffic in Transit* WT/DS512/R 5 April 2019 (*Russia – Traffic in Transit*).

[93]*Russia – Traffic in Transit*, paras. 7.102–7.104.

[94]Westin (1997), pp. 181–182; Jackson (1989), p. 205, Article XXI Security Exceptions, WTO Analytical Index of the GATT, at 600–601, https://www.wto.org/english/res_e/booksp_e/gatt_ai_e/art21_e.pdf.

[95]Westin (1997), pp. 181–182; Jackson (1989), p. 205, Article XXI Security Exceptions, WTO Analytical Index of the GATT, at 600–601, https://www.wto.org/english/res_e/booksp_e/gatt_ai_e/art21_e.pdf.

legal meaning of the adjectival clause "which it considers" allows a WTO member *itself* to determine "the 'necessity' of the measures for the protection of its essential security interests."[96] This "necessity test" is therefore easier to satisfy than the "necessity test" of the general exception. As the WTO Panel in *Russia – Traffic in Transit* clarified, to satisfy the "necessity test" in the national security exception

> there is no need to determine the extent of the deviation of the challenged measure from the prescribed norm in order to evaluate the necessity of the measure, i.e. that there is no reasonably available alternative measure to achieve the protection of the legitimate interests covered by the exception which is not violative, or is less violative, of the prescribed norm.[97]

The recent WTO Panel decision, however, also confirms that the breadth of the margin of appreciation in determining "necessity" in the national security exception is limited by the obligation to interpret and apply the exception in good faith, a general principle of law and a principle of general international law.[98] This means that a WTO member cannot use the security exception "as a means to circumvent their obligations under the GATT 1994."[99] In other words, by means of interpretation the WTO Panel implicitly injected the general exception's chapeau requirements, which are absent in the wording of the national security exception.

This analysis suggest that the model clauses aim to provide for a bullet-proof protection for the EU's regime for transfers of personal data under the GDPR from any possible review by trade adjudicators. At the same time, the clauses are not out of the woods yet as they only represent a starting point in negotiations. It may be difficult for the EU to convince its trading partners to accept the proposal for at least two reasons. First, some of them, such as Indonesia, are in the process of adopting data localization rules.[100] Second, other trading partners, like Australia and New Zealand are already parties to CPTPP which, as the next section demonstrates, implements an entirely different—US—approach. Even if the EU model provisions are included in the actual FTAs, their effectiveness could be diminished due to remaining uncertainty on the relationship between the specific exception for privacy and data protection in these provisions and the general exception for privacy and data protection in the services chapter. Although the model exception is clearly intended as *lex specialis* as opposed to the *lex generalis* of the general exception for privacy and data protection, a trading partner could still argue that the general exception should apply when the EU restrictions on cross-border transfers of

[96] *Russia – Traffic in Transit*, para. 146. Before this decision was adopted, scholars were sharply divided on whether the national security is self-judging. Compare Alford (2011), pp. 701–702 with Schloemann and Ohlhoff (1999), pp. 426–427, 438, 443ff, arguing that it is not.

[97] *Russia – Traffic in Transit*, para. 7.108.

[98] *Russia – Traffic in Transit*, para. 7.132. Several scholars made the same argument before this decision was adopted. See e.g. Schloemann and Ohlhoff (1999), pp. 446–447.

[99] *Russia – Traffic in Transit*, para. 7.133.

[100] Herbert Smith Freehills LLP, Indonesia proposes amendments to its data localisation requirement, Lexology, 11 December 2018, https://www.lexology.com/library/detail.aspx?g=a116020b-cee3-433f-b62b-a5e988477d8e.

personal data are challenged as violating a non-discrimination provision in trade in services (and not the digital trade provisions) and by doing so by-pass the national security-type exception.

5.2 *The US Approach to Privacy and Data Protection in Digital Trade Chapters*

The US approach to digital trade ingrains the country's regulatory model of privacy and data protection. The obligation not to restrict cross-border data flows, an exception from such provision and an article on the protection of personal information included in the CPTPP, USMCA, U.S. – Japan Digital Trade Agreement and the US proposal for WTO negotiations on electronic commerce[101] reflect the US regulatory preference for free cross-border data flows and an economic—as opposed to fundamental rights—approach to the protection of personal information in commercial sphere.[102]

CPTPP and USMCA are the first FTAs, which contain a binding provision requiring each Party to allow (or not to restrict) 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.[103] Both FTAs also contain an exception which allows the Parties to adopt or maintain measures inconsistent with this obligation 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* [*necessary*—in the USMCA] to achieve the objective. (emphasis added)[104]

The structure and text of the exception strongly resembles the general exception of Article XIV (c) of the GATS, but are nevertheless different in two respects. First, instead of the "necessity" requirement in the general exception, the CPTPP exception requires that restrictions should not be "greater than are *required* to achieve the objective". This difference seems, however, purely semantic. "Required" is a synonym of "necessary"[105] and, according to the WTO Secretariat is yet another way to

[101] Manak I., U.S. WTO E-commerce Proposal Reads Like USMCA, International Economic Law and Policy Blog, 8 May 2019, https://worldtradelaw.typepad.com/ielpblog/2019/05/us-wto-e-commerce-proposal-reads-like-usmca.html.

[102] Wolfe (2019), pp. s75 and s77. For a comparison between EU and US approaches to privacy and data protection see Schwartz and Solove (2014).

[103] Article 14.11(2) of CPTPP, article 19.11(1) of USMCA.

[104] Article 14.11 (3) of CPTPP. Article 19.11(2) of USMCA contains an almost identical provision.

[105] Merriam-Webster online dictionary, https://www.merriam-webster.com/dictionary/necessary.

convey the concept of "necessity."[106] Second, as compared with the general exception, exceptions from the obligation on cross-border data flows do not explicitly name public policy objective that could trigger its application. It could be reasonably argued that privacy and data protection constitute the policy objectives implied in the CPTPP and USMCA exceptions. However, unlike the EU' model exception, these policy objectives are not limited to privacy and data protection. To sum up, while the exception in CPTPP and USMCA embraces an unrestricted scope of public policy objectives, by incorporating the "necessity test" of the general exception it allows for a sufficiently narrower regulatory autonomy to pursue those objectives than the national security-type exception proposed by the EU.

Another novelty introduced in the CPTPP and later in the USMCA is an extensive article on the protection of personal information.[107] Article 14.8 "Personal Information Protection" in the CPTPP includes a mixture of binding and aspirational provisions:

i. An aspirational provision recognising the economic and social benefits of protecting personal information in the context of digital trade (para. 1);
ii. An obligation to ("each Party shall") adopt or maintain a legal framework for protection of personal data of users of electronic commerce and to consider principles and guidelines of relevant international bodies (para. 2);
iii. An aspirational provision to adopt non-discriminatory practices in protecting the users' personal information (para. 3);
iv. An obligation to ("each Party should") publish information on how individuals can pursue a remedy in case of violation of personal information protections and on how business can comply with the local personal information protection requirements (para. 4);
v. An aspirational provision requiring to encourage the development of mechanisms ensuring compatibility between different data protection regimes, such as recognition of regulatory outcomes and to endeavour to exchange information on such mechanisms (para. 5).

Article 19.8 of the USMCA, which incorporates all the provisions mentioned above, is different in two important aspects. First, it endorses the APEC Privacy Framework and the 2013 OECD Guidelines governing the Protection of Privacy and Transborder Flows of Personal data as examples of such framework as an example of a legal framework for the protection of personal information (para. 2). Second, paragraph 3 explicitly lists the key principles of the personal information framework: limitation on collection; choice; data quality; purpose specification; use limitation; security safeguards; transparency; individual participation; and accountability. Furthermore, this paragraph embraces a Parties' recognition of the importance to ensure that "any restrictions on cross-border flows of personal information are necessary and proportionate to the risks presented."

[106]WTO, Note by the Secretariat, '"Necessity" in the WTO', S/WPDR/W/27, 2 December 2003, para. I.A.5.
[107]Article 14.8 of CPTPP and article 19.8 of USMCA.

On the one hand, these articles remotely resemble the provisions included in the EU's e-commerce chapters, discussed in Sect. 4 of this chapter (especially provisions (i) and (ii)), which are not present in JEFTA, and the model clauses on cross-border data flows discussed in Sect. 5.1 above. On the other hand, they go a step further by incorporating—for the first time in international trade law—substantive principles of US personal information protection. Another important novelty is an emphasis on developing mechanisms for compatibility between different data protection regimes (provision v) supported by a transparency obligation (provision iv). In addition to its, perhaps, primary function of facilitating cross-border digital trade, the latter obligation can also serve an important starting point for the trading partners to learn about each other's legal regimes for personal data protection in commerce.

6 Conclusion

The analysis of international trade provisions in EU- and US-led post-WTO FTAs referring to privacy and data protection confirms that, apart from the wording of the general exception, both trading partners tend to prefer their own template for regional FTAs.[108] Comparison of these templates demonstrates that they are rooted in domestic regulatory models of information governance, which, in particular, embrace normative underpinnings for privacy and data protection. In addition, each of the trading partners respond differently to particular business demands.[109] This chapter also showed that compared to the EU, the US template for provisions mentioning privacy and data protection in telecommunications and financial services chapters, e-commerce and digital trade chapters has been internally more coherent and aligned with the WTO Agreement.

Returning to digital trade, it could be argued that both the EU and the US attempt to harmonize the standards for cross-border transfers and the protection of privacy and personal data using their own regulatory model as a benchmark.[110] For example, the EU's model provision prohibiting restrictions on cross-border data flows is carefully crafted to outlaw data localization measures adopted by, for example, Russia and China. The US, in its turn, aims to set the level of data protection at a level lower than that in the EU, aligned with its own market-based approach to data protection.

Against this backdrop, convergence of the EU and US models is unlikely. Although some predict[111] and others even consider desirable[112] the diffusion of

[108]Wolfe (2019), p. s66.

[109]Wolfe (2019), p. s65.

[110]Bradford (2012), p. 22ff. In contrast, Young disagrees that the EU is exporting its regulatory model. Young (2015), p. 1255.

[111]Burri (2017a), p. 128.

[112]Mattoo and Meltzer (2018), pp. 5–6 and 25.

the CPTPP template for cross-border data flow provisions in international trade agreements, the EU is unlikely to adhere to it as this would require compromising on its constitutional legal regime for privacy and data protection.[113] This may be problematic for other countries, such as Japan or Canada. On the one hand, Japan and Canada are parties to the CPTPP; Canada is party to USMCA and Japan to the U.S. – Japan Digital Trade Agreement modelled after the digital trade provisions in the USMCA. These FTAs provide for a broad prohibition on restrictions on cross-border data flows. On the other hand, both Japan and Canada have an adequacy decision from the EU, which among other things require limitations on onward transfers of personal data obtained from the EU to other countries, which have not been granted adequacy, such as the US (beyond the EU-US Privacy Shield certification mechanism[114]) or Australia. Mutual inconsistency of the EU and US approaches to cross-border data flows and the protection of privacy and personal data may prove counterproductive in the multilateral negotiations on electronic commerce at the WTO.[115] Finding a common ground on data protection could allow the two trading partners to strengthen their negotiating power and offset that of less democratic states, such as China.[116]

References

Aaronson SA (2016) Redefining protectionism. Int Econ 30(4):58–88

Alford RP (2011) The self-judging WTO security exception. Utah Law Rev 2011(3):697–759

Bradford A (2012) The Brussels effect. Northwest Univ Law Rev 107(1):1–68

Burri M (2017a) The governance of data and data flows in trade agreements: the pitfalls of legal adaptation. UC Davis Law Rev 51(65):65–132

Burri M (2017b) Current and emerging trends in disruptive technologies: implications for the present and future of EU's trade policy. Study commissioned by the European Parliament's Committee on International Trade, 1–37 http://www.europarl.europa.eu/RegData/etudes/STUD/2017/603845/EXPO_STU(2017)603845_EN.pdf

Cottier T, Delimatsis P (2008) Article XIVbis security exceptions. In: Wolfrum R, Stoll PT, Feinäugle C (eds) Max Planck commentaries on world trade law, WTO – trade in services, vol 6. Martinus Nijhoff, Leiden, pp 329–348

Irion K, Yakovleva S, Bartl M (2016) Trade and privacy: complicated bedfellows? How to achieve data protection-proof free trade agreements. Study commissioned by BEUC et al. Institute for Information Law (IViR), Amsterdam

Jackson J (1989) The world trading system: law and policy of international economic relations. MIT Press, Cambridge MA

[113] Yakovleva and Irion (2020).

[114] European Commission implementing decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on adequacy of the protection provided by the EU-U.S. Privacy Shield of 12.07.2016 C(2016) 4176 final.

[115] Yakovleva and Irion (2020), p. 14.

[116] Yakovleva and Irion (2020), p. 14.

Le Roux G (2017) TTIP negotiations, policy convergence, and the transatlantic digital economy. Bus Polit 19(4):709–737
LeSieur F (2012) Regulating cross-border data flows and privacy in the networked digital environment and global knowledge economy. Int Data Privacy Law 2(2):93–104
Mattoo A, Meltzer JP (2018) International data flows and privacy the conflict and its resolution, policy research working paper 8431. World Bank Group, Washington D.C.
Monteiro JA, Teh R (2017) Provisions on electronic commerce in regional trade agreements. WTO working paper ERSD-2017-11. ERSD, Geneva
Regan DH (2007) The meaning of "necessary" in GATT Article XX and GATS Article XIV: the myth of cost-benefit balancing. World Trade Rev 6(3):347–369
Rodota S (2009) Data protection as fundamental right. In: Gutwirth S et al (eds) Reinventing data protection? Springer, Heidelberg, pp 77–82
Schloemann HL, Ohlhoff S (1999) Constitutionalization and dispute settlement in the WTO: national security as an issue of competence. Am J Int Law 93(2):424–451
Schwartz PM, Solove DJ (2014) Reconciling personal information in the United States and European Union. Calif Law Rev 102(4):877–916
Shaffer G (2000) Globalization and social protection: the impact of EU and international rules in the ratcheting up of U.S. privacy standards. Yale J Int Law 25(1):1–88
Svantesson DJB (2011) The regulation of cross-border data flows. Int Data Privacy Law 1 (3):180–198
Swire P, Litan RE (1998) None of your business: world data flows, electronic commerce, and the European Privacy Directive. Brookings Institution Press, Washington
Venzke I (2011) Making general exceptions: the spell of precedents in developing Article XX GATT into standards for domestic regulatory policy. German Law J 12(05):1111–1140
Westin RA (1997) Environmental tax initiatives and multilateral trade agreements: dangerous collisions. Kluwer Law International, Alphen aan den Rijn
Wolfe R (2019) Learning about digital trade: privacy and e-commerce in CETA and TPP. World Trade Rev 18(S1):s63–s84
Wunsch-Vincent S (2003) The digital trade agenda of the U.S.: parallel tracks of bilateral, regional and multilateral liberalization. Aussenwirtschaft 58(I):7–46
Yakovleva S (2018) Should fundamental rights to privacy and data protection be a part of EU's international trade "deals"? World Trade Rev 17(3):477–508
Yakovleva S (2020) Privacy protection(ism): the latest wave of trade constraints on regulatory autonomy. University of Miami Law Review 416
Yakovleva S, Irion K (2020) Towards compatibility of the EU external trade policy on cross-border data flows with the general data protection regulation. Am J Int Law Unbound 114:10–14. Symposium on the GDPR and International Law
Young AR (2015) Liberalizing trade, not exporting rules: the limits to regulatory co-ordination in the EU "New Generation" preferential trade agreements. J Eur Public Policy 22(9):1253–1275

Svetlana Yakovleva is a PhD candidate at the Institute for Information Law (IViR) of the University of Amsterdam. She also works part-time as a Senior Legal Adviser in Privacy and Cybersecurity practice group at De Brauw Blackstone Westbroek in Amsterdam. Her primary research interests lie at the intersection of data privacy and cybersecurity law, human rights and international trade law. Svetlana received a degree in law (cum laude) from the National Research University Higher School of Economics (Moscow) in 2005. She also holds an LL.M degree in Law and Economics (EMLE) from the Erasmus University, Rotterdam and the University of Hamburg (2007), and a research master degree in Information law from the IViR (2016). Between 2007 and 2014, Svetlana worked as a trainee lawyer at the Moscow office of Debevoise&Plimpton LLP, independent legal counsel and Legal and Compliance Officer at Allianz Global Assistance Russia. Svetlana also provided legal and methodological advice for the e-Government project of the Russian Government.