SCHOOL OF LAW
CASE WESTERN RESERVE UNIVERSITY

Case Western Reserve Journal of International Law

Volume 53 | Issue 1 Article 5

2021

Interfacing Privacy and Trade

Mira Burri

Follow this and additional works at: https://scholarlycommons.law.case.edu/jil

 Part of the International Law Commons

Recommended Citation

Mira Burri, *Interfacing Privacy and Trade*, 53 Case W. Res. J. Int'l L. 35 (2021)
Available at: https://scholarlycommons.law.case.edu/jil/vol53/iss1/5

This Article is brought to you for free and open access by the Student Journals at Case Western Reserve University School of Law Scholarly Commons. It has been accepted for inclusion in Case Western Reserve Journal of International Law by an authorized administrator of Case Western Reserve University School of Law Scholarly Commons.

INTERFACING PRIVACY AND TRADE

Mira Burri[*]

TABLE OF CONTENTS

A. INTRODUCTION: THE INCREASINGLY CONTENTIOUS NATURE OF THE TRADE AND PRIVACY INTERFACE

Privacy and trade law have developed independently from each other, as their objectives and the tools of achieving those objectives are profoundly different. Privacy protection can be framed as an individual right, as the article explains in more detail below, while trade law enables the flow of goods, services, capital, and less so of people across borders.[1] While both have their origins in the aftermath of World War

* Mira Burri is a Senior Lecturer at the Faculty of Law of the University of Lucerne, Switzerland. She is also the Principal Investigator of the research project "The Governance of Big Data in Trade Agreements."

1. *See, e.g.*, M. Elizabeth Smith, *The Public's Need for Disclosure v. The Individual's Right to Financial Privacy: An Introduction to the Financial Right to Privacy Act of 1978*, 32 ADMIN. L. REV. 511, 513 (1980); William M. Beaney, *The Right to Privacy and American Law*, 31 L. & CONTEMP. PROBLEMS 253, 254 (1966).

II,[2] with one providing for individual rights' protection against the state[3] and the other securing peace by regulating economic relations,[4] the rule-frameworks and the institutions created in the two domains are very different. The interfaces between privacy protection and trade law and the underlying tensions between sovereignty and international cooperation have not been common for a long time; neither have they been addressed in the legal frameworks.[5] The topic of privacy has not been one of the classic trade law treatises,[6] and privacy textbooks have equally rarely thought of trade law.[7] While there has been a robust scholarly and policy debate on the impact of the "hard" rules of international economic law on non-economic interests,[8] privacy has seldom been one of the major concerns and fields of contestation.[9]

2. *See* Robert E. Baldwin, *The Changing Nature of U.S. Trade Policy Since WWII*, *in* THE STRUCTURE AND EVOLUTION OF RECENT U.S. TRADE POLICY 5, 15–16 (Robert E. Baldwin & Anne O. Krueger eds., 1984).

3. *See, e.g.*, PHILIP ALSTON & RYAN GOODMAN, INTERNATIONAL HUMAN RIGHTS 148 (2012).

4. *See, e.g.*, Thomas Cottier, *The Legitimacy of WTO*, *in* THE LAW AND ECONOMICS OF GLOBALISATION 11–48 (Linda Y. Yueh ed., 2009).

5. The General Agreement on Tariffs and Trade (GATT) 1947 makes no reference to privacy and most of the free trade agreements up to very recently make no mention of it. *See, e.g.*, Graham Greenleaf, *Looming Free Trade Agreements Pose Threats to Privacy*, 152 PRIVACY L. & BUS. INT'L REP. 23, 23 (2018).

6. *See, e.g.*, JOHN H. JACKSON, THE WORLD TRADING SYSTEM: LAW AND POLICY OF INTERNATIONAL ECONOMIC RELATIONS (2ND ED. 1989); JOHN H. JACKSON ET AL., LEGAL PROBLEMS OF INTERNATIONAL ECONOMIC RELATIONS (6th ed. 2013); JOHN H. JACKSON, THE WORLD TRADE ORGANIZATION: CONSTITUTION AND JURISPRUDENCE (1998); WTO – TRADE IN GOODS (Rüdiger Wolfrum et al. eds., 2011).

7. *See, e.g.*, DANIEL J. SOLOVE & PAUL SCHWARTZ, INFORMATION PRIVACY LAW (7th ed. 2014); THE EU GENERAL DATA PROTECTION REGULATION: A COMMENTARY (Christopher Kuner et al. eds., 2020).

8. *See, e.g.*, Andrew T. F. Lang, *Reflecting on "Linkage": Cognitive and Institutional Change in The International Trading System*, 70 THE MODERN L. REV. 523, 548 (2007); INTERNATIONAL TRADE AND HUMAN RIGHTS: FOUNDATIONS AND CONCEPTUAL ISSUES (Frederick M. Abbott et al. eds., 2006); THE WTO AND LABOR AND EMPLOYMENT (Drusilla K. Brown & Robert M. Stern eds., 2007); RESEARCH HANDBOOK ON ENVIRONMENT, HEALTH AND THE WTO (Geert Van Calster & Denise Prévost eds., 2013); RESEARCH HANDBOOK ON CLIMATE CHANGE AND TRADE LAW (Panagiotis Delimatsis ed., 2016).

9. *But see, e.g.*, Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards*, 25 YALE J. INT'L L. 1, 4 (2000); Gregory Shaffer, *Reconciling Trade and Regulatory Goals: The Prospects and Limits of New Approaches to Transatlantic Governance through Mutual Recognition and Safe Harbor Agreements*, 9 COLUM. J. EUR. L. 29, 29 (2002).

The interface between trade and privacy protection became relevant because of technological advances, which permitted the easy flow of information across borders and exposed the existing tensions.[10] During the late 1970s and the 1980s, as satellites, computers and software changed the dynamics of communications, the trade-offs between allowing data to flow freely and asserting national jurisdiction became readily apparent.[11] Some states, echoing the concerns of large multinational companies, started to worry that barriers to information flows may seriously hinder economic activities and thus looked for mechanisms that could prevent the erection of such barriers.[12] It was clear that some sort of a balancing mechanism was needed. Such a mechanism was found, in a soft legal form, in the principles elaborated under the auspices of the Organisation for Economic Co-operation and Development ("OECD").[13] However, the OECD framework, which is briefly discussed later in this article, provided the bare minimum and readily permitted diverging approaches of data protection, such as those of the European Union ("EU") and the United States ("US").[14] Moreover, as the OECD itself points out, while this privacy framework endured, the situation in the 1970s and 1980s is profoundly different from the challenges in the realm of data governance we face today.[15] Pervasive digitization and powerful hardware, coupled with the societal embeddedness of the Internet, have changed the volume, the intensity, and the nature of data flows.[16]

10. *See, e.g.*, Christopher Kuner, *Regulation of Transborder Data Flows Under Data Protection and Privacy Law: Past, Present and Future*, 8 (OECD Digital Economy Papers, Working Paper No. 187, 2011); Susan Aaronson, *Why Trade Agreements Are Not Setting Information Free: The Lost History and Reinvigorated Debate Over Cross-Border Data Flows, Human Rights and National Security*, 14 WORLD TRADE REV. 671, 672 (2015).

11. Aaronson, *supra* note 10, at 672.

12. *Id.* at 673–74.

13. *Guidelines for the Protection of Personal Information and Transborder Data Flows of Personal Data* ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT [OECD] (Sept. 23, 1980), https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm [https://perma.cc/A44T-RTF4].

14. *Id.*

15. ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT [OECD], *The OECD Privacy Framework* (2013), http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf [https://perma.cc/3H2D-R6RE] [hereinafter OECD, *Privacy Framework*].

16. *See* James Manyika et al., *Big Data: The Next Frontier for Innovation, Competition, and Productivity*, MCKINSEY INST. (June 2011), https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Big%20data%20The%20next%20f

The value of data and Big Data,[17] as well as the risks associated with data collection, data processing, its use and re-use — by both companies and governments — has dramatically changed. On one hand, data has become so essential to economic processes that it is considered the "new oil."[18] Although this concept is flawed, since data is not exhaustible and may lose its usefulness over time,[19] it aptly shows the high value associated with it. Like other factors of production, such as natural resources and human capital, it appears that much of modern economic activities, innovation and growth cannot occur without data.[20] Emerging technologies, like Artificial Intelligence ("AI"), are highly dependent on data inputs as well, so the future of the data-driven economy is, in many aspects, at stake.[21] Many studies have

rontier%20for%20innovation/MGI_big_data_full_report.pdf [https://perma.cc/KG5U-VGEB]; VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK (2013); Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904 (2013); Neil M. Richards & Jonathan H. King, *Big Data Ethics*, 49 WAKE FOREST L. REV. 393 (2014).

17. There are no clear definitions of small versus Big Data. Definitions vary and scholars seem to agree that the term of Big Data is generalized and slightly imprecise. One common identification of Big Data is through its characteristics of volume, velocity, and variety, also referred to as the "3-Vs." Increasingly, experts add a fourth "V" that relates to the veracity or reliability of the underlying data and fifth one with regard to its value. *See* MAYER-SCHÖNBERGER & CUKIER, *supra* note 16, at 13. For a brief introduction to Big Data applications and review of the literature, see Mira Burri, *Understanding the Implications of Big Data and Big Data Analytics for Competition Law: An Attempt for a Primer*, *in* NEW DEVELOPMENTS IN COMPETITION BEHAVIOURAL LAW AND ECONOMICS 241–263 (Klaus Mathis & Avishalom Tor eds., 2019).

18. David Parkins, *The World's Most Valuable Resource Is No Longer Oil, But Data*, THE ECONOMIST (May 6, 2017) https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data https://perma.cc/K8FZ-DFQP].

19. Amongst other arguments, see Burri, *supra* note 17, for a full analysis; *see* Lauren Henry Scholz, *Big Data Is Not Big Oil: The Role of Analogy in the Law of New Technologies*, 86 TENN. L. REV. 863 (2019).

20. Manyika et al., *supra* note 16.

21. *See* Kristina Irion & Josephine Williams, *Prospective Policy Study on Artificial Intelligence and EU Trade Policy*, AMSTERDAM: THE INST. FOR INFO. L., 31–32 (2019); *see generally* The Royal Society, *Machine Learning: The Power and Promise of Computers That Learn by Example* (2017); Anupam Chander, *Artificial Intelligence and Trade*, *in* BIG DATA AND GLOBAL TRADE LAW 115–127 (Mira Burri ed., 2021).

revealed the vast potential of data,[22] and companies as well as governments are seeking to realize this potential.[23]

On the other hand, increased dependence on data has brought about a new set of concerns. Scholars and policymakers alike have widely acknowledged the impact of data collection and its use upon privacy as has been felt by regular users of digital products and services.[24] The risks have only been augmented in the era of Big Data and AI, which presents certain distinct challenges to the protection of personal data and by extension to the protection of personal and family life.[25] For example, Big Data questions the very distinction between personal and non-personal data as citizens become "transparent."[26] On one hand, it appears that one of the basic tools of data protection — that of anonymization, i.e. the process of removing identifiers to create anonymized datasets — is only of limited utility in a data-driven world, as it is now rare for data generated by user activity to be completely

22. *See, e.g.*, Manyika et al., *supra* note 16; MAYER-SCHÖNBERGER & CUKIER, *supra* note 16; Nicolaus Henke et al., *The Age of Analytics: Competing in a Data-Driven World,* MCKINSEY GLOBAL INSTITUTE (Dec. 2016) https://www.mckinsey.com/~/media/McKinsey/Industries/Public%20and%20Social%20Sector/Our%20Insights/The%20age%20of%20analytics%20Competing%20in%20a%20data%20driven%20world/MGI-The-Age-of-Analytics-Full-report.pdf [https://perma.cc/9W6E-G3K4].

23. *See, e.g.*, Manyika et al., *supra* note 16; Henke et al., *supra* note 22; Jacques Bughin et al., *Digital Europe: Pushing the Frontier, Capturing the Benefits*, MCKINSEY GLOB. INST. (Dec. 2016) https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/digital%20europe%20pushing%20the%20frontier%20capturing%20the%20benefits/digital-europe-full-report-june-2016.ashx [https://perma.cc/2DSF-NSRQ].

24. Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1766–67 (2010); Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1854 (2011); Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 NW. J. OF TECH. AND INTELL. PROP. 239, 264 (2013); John Podesta et al., *Big Data: Seizing Opportunities, Preserving Values*, EXECUTIVE OFFICE OF THE PRESIDENT, (May 2014) https://www.hsdl.org/?abstract&did=752636 [https://perma.cc/K42N-UXFA]; Urs Gasser, *Recoding Privacy Law: Reflections on the Future Relationship Among Law, Technology, and Privacy*, 130 HARV. L. REV. 61, 65 (2016). *See* Colin J. Bennett & Robin M. Bayley, *Privacy Protection in the Era of 'Big Data': Regulatory Challenges and Social Assessments*, *in* EXPLORING THE BOUNDARIES OF BIG DATA 205, 215–23 (Bart van der Sloot et al. eds., 2016); Sheri B. Pan, *Get to Know Me: Protecting Privacy and Autonomy Under Big Data's Penetrating Gaze*, 30 HARV. J. OF L. & TECH. 239, 244 (2016).

25. *See, e.g.*, Ohm, *supra* note 24, at 1748.

26. Joel R. Reidenberg, *The Transparent Citizen*, 47 LOYOLA UNIV. CHICAGO L. J. 437, 438–48 (2015).

and irreversibly anonymized.[27] On the other hand, Big Data analytics enable the re-identification of data subjects by combining datasets of non-personal data, especially as data is persistent and can be retained indefinitely.[28] Big Data also casts doubt on the efficacy of existing privacy protection laws, which often operate upon requirements of transparency and user consent.[29] Data minimization is another core idea of privacy protection that has been challenged, as firms are "hungry" to get hold of more data, and the sources of data from smart devices, sensors, and social networks' interactions multiply.[30] These challenges are not unnoticed and have triggered the reform of data protection laws around the world, best evidenced by the EU's General Data Protection Regulation ("GDPR").[31] However, these reform initiatives are not coherent and are culturally and socially embedded, reflecting societies' deep understandings of constitutional values, relationships between citizens and the state, and the role of the market, as illustrated with a discussion of the differences in approaches between the US and the EU to data protection that follows later in this article.

The tensions around data have also revived older questions about sovereignty and international cooperation in cyberspace.[32] Although there has been an agreement, as maintained in the *Tallinn Manual 2.0 on the International Law Applicable to Cyber-Operations ("Tallinn 2.0"),*[33] that cyberspace does not change the nature of jurisdiction and "[s]ubject to limitations set forth in international law, a State may

27. Podesta et al., *supra* note 24; *Guidelines for Data De-Identification or Anonymization*, EDUCASE https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/resources/information-security-guide/toolkits/guidelines-for-data-deidentification-or-anonymization [https://perma.cc/4DQK-H2FT].

28. Podesta et al., *supra* note 24, at 14–15; *see also* Ohm, *supra* note 24, at 1704; Ira S. Rubinstein, *Big Data: The End of Privacy or a New Beginning?*, 3 INT'L DATA PRIV. L. 74, 77 (2013).

29. Rubinstein*, supra* note 28, at 78.

30. Tene & Polonetsky, *supra* note 24, at 241.

31. Regulation 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), O.J. (L 119) 1 [hereinafter GDPR].

32. For a great review of the theories on cyberspace regulation, their evolution over time and review of the literature, see Kristen E. Eichensehr, *The Cyber-Law of Nations*, 103 GEO. L. J. 317, 331–34 (2015).

33. *See generally* INTERNATIONAL GROUP OF EXPERTS AT THE INVITATION OF THE NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE, TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER-OPERATIONS (Michael N. Schmitt ed., 2nd ed., 2017). *See also* Eric T. Jensen, *The Tallinn Manual 2.0: Highlights and Insights*, 48 GEO. J. INT'L L. 736, 746–60 (2017).

exercise territorial and extraterritorial jurisdiction over cyber activities,"[34] the application of this rule has not been easy in practice.[35] As the *Tallinn 2.0* drafters themselves pointed out, "determining whether enforcement jurisdiction is territorial or extraterritorial can be complex in the cyber context"[36] and the nature of data and data flows only exacerbate this problem.[37] Data's intangibility and pervasiveness pose particular difficulties for determining where data is located, as bits of data, even those associated with a single transaction or online activity, can be located anywhere.[38] Even in relatively straightforward situations, where the data is simply located on a server abroad, the application of national law can be tricky, as clearly demonstrated by *US v. Microsoft*.[39] The extraterritorial application of court judgments can also be highly problematic, as illustrated by some well-known decisions by the Court of Justice of the European Union ("CJEU"), such as *Google Spain*,[40] and more recently, *Glawischnig-Piesczek v.*

34. *See* INTERNATIONAL GROUP OF EXPERTS AT THE INVITATION OF THE NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE, *supra* note 33, at 51.

35. *See, e.g.*, Kristen E. Eichensehr*, Data Extraterritoriality*, 95 TEX. L. REV. 145 (2017).

36. INTERNATIONAL GROUP OF EXPERTS AT THE INVITATION OF THE NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE, *supra* note 33, at 69.

37. *See id.*

38. *See, e.g.*, Eichensehr, *supra* note 35, at 145.

39. United States v. Microsoft Corp. 584 U.S. _____, 138 (2018) was a data privacy case involving the extraterritoriality of law enforcement seeking electronic data under the 1986 Stored Communications Act (SCA), Title II of the Electronic Communications Privacy Act of 1986, *id.* In 2013, Microsoft challenged a warrant by the federal government to turn over email of a target account that was stored in Ireland, arguing that a warrant issued under Section 2703 of the SCA could not compel US companies to produce data stored in servers abroad, *id.* Microsoft initially lost in the Southern District of New York, with the judge stating that the nature of the Stored Communication Act warrant, as passed in 1986, was not subject to territorial limitations, *id.* Microsoft appealed to the US Court of Appeals for the Second Circuit, who found in favor of Microsoft and invalidated the warrant in 2016, *id.* In response, the Department of Justice appealed to the Supreme Court of the United States, which decided to hear the appeal, *id.* While the case was pending, Congress passed the Clarifying Lawful Overseas Use of Data Act (CLOUD Act), which amended the SCA to resolve concerns from the government and Microsoft related to the initial warrant. The US Supreme Court, following agreement from the government and Microsoft, determined the passage of the CLOUD Act and a new warrant for the data filed under it made the case moot and vacated the Second Circuit's decision.

40. Case C-131/12, Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González,

Facebook,[41] as well as the *Equustek* decision from the Supreme Court of Canada.[42]

With the increased value of data, the associated risks, and contentious jurisdictional issues, governments have sought new ways to

ECLI:EU:C:2014:317 (May 13, 2014). The *Google Spain* case coined the infamous "right to be forgotten." Under the 1995 EU Data Protection Directive, the CJEU ruled that a search engine is regarded as a "controller" with respect to "processing" of personal data through its act of locating, indexing, storing, and disseminating such information. It also held that in order to guarantee the rights of privacy and the protection of personal data, search engines operators can be required to remove personal information published by third party websites. In a follow-up judgement, the CJEU did limit the geographic scope of the "right to be forgotten" and help that it should be applicable to EU citizens. *See* Case C-507/17, Google LLC v. Commission nationale de l'informatique et des libertés (CNIL), ECLI:EU:C:2019:772 (Sept. 24, 2019).

41. Case C-18/18, Eva Glawischnig-Piesczek v. Facebook Ireland Limited, ECLI:EU:C:2019:821 (Oct., 3, 2019). This is a defamation case that was about the liability of intermediaries. The case arose in 2016 when an anonymous Facebook user shared an article and a defamatory comment against the applicant Eva Glawischnig–Piesczek, an Austrian Green Party politician. The case was referred to the CJEU, which found that the E-Commerce Directive does not preclude a Member State from ordering a hosting provider to remove or block content that has been declared unlawful, or content that is identical or equivalent to such unlawful information. The Court also held that the Directive does not preclude Member states from ordering such removal worldwide, and therefore left it to the Member States to determine the geographic scope of the restriction within the framework of the relevant national and international laws.

42. Google Inc. v. Equustek Solutions Inc., [2017] 1 S.C.R. 824 (Can.). This is an IP case, where the Court found that Canadian courts could grant a global injunction against a non-party to litigation when the order is fair and equitable in the circumstances of the case, *id.* The Supreme Court was unconvinced by Google's arguments that a global de-indexing order would offend international comity, would unreasonably inconvenience the search engine, and would interfere with the right to freedom of expression, *id.* The case is now being continued in the US, where the US District Court of Northern California granted Google a temporary injunction blocking the enforceability of the Supreme Court of Canada's order in the United States. *See, e.g.*, Alica Loh, *Google v. Equustek: United States Federal Court Declares Canadian Court Order Unenforceable*, JOLT DIGEST, HARV. L. (Nov. 16, 2017), https://jolt.law.harvard.edu/digest/google-v-equustek-united-states-federal-court-declares-canadian-court-order-unenforceable [https://perma.cc/W7EH-ESVF]. The California Court granted the injunction on the basis that the company was protected as a neutral intermediary under Section 230 of the Communications Decency Act 1996, *id.* It also said that "the Canadian order undermines the policy goals of Section 230 and threatens free speech on the global internet." Google LLC v. Equustek Sols. Inc., No. 5:17-cv-04207-EJD, 2017 U.S. Dist. LEXIS 182194, at *8 (N.D. Cal., Nov. 2, 2017). It is expected that Google will apply to make the injunction permanent.

assert control over it — in particular by prescribing diverse measures that "localize" the data to keep it within one state's sovereign space.[43] However, erecting barriers to data flows impinges directly on trade and may also endanger the realization of an innovative data economy.[44] The provision of any digital products and services, cloud computing applications, or the development of the Internet of Things ("IoT") and AI are impossible under restrictions on cross-border flows of data.[45] Data protectionism may also be associated with certain costs for the economy that endorses it.[46]

Overall, with the increased role of data in societies, the interfaces between trade and privacy protection have grown and intensified, thus raising important questions regarding adequate regulatory design that reconciles economic and non-economic concerns along with national and international interests. This article is set against this complex backdrop and seeks to provide a better understanding and contextualization of the theme of data protection and its interfaces with global trade law. First, this article looks at the existing international, transnational, and selected national frameworks for privacy protection and their evolution over time. The article then explores the application of the rules of the World Trade Organization ("WTO") to situations where privacy concerns may be affected. This article then looks at the data-relevant and data protection rules that have emerged in preferential trade venues with a focus on reconciliation mechanisms. Finally, the article concludes with some thoughts on the pros and cons of the available legal solutions for reconciling trade and privacy protection and provides an outlook on this contentious relationship and its possible resolution.

43. *See* Anupam Chander, *National Data Governance in a Global Economy*, 495 UC DAVIS L. STUD. RSCH. PAPER 1, 2 (2016); *see also* Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 EMORY L. J. 677, 690 (2015).

44. Digital Trade in the US and Global Economies, Part 1, Inv. No. 332–531, USITC Pub. 4415 (July 2013); Digital Trade in the US and Global Economies, Part 2, Inv. No. 332–540, USITC Pub. 4485 (Aug. 2014). For a country survey, see Chander & Lê, *supra* note 43.

45. *See* Chander, *supra* note 43, at 2.

46. *See, e.g.*, Martina F. Ferracane, *The Costs of Data Protectionism*, (Oct. 25, 2018), https://voxeu.org/article/cost-data-protectionism [https://perma.cc/D7W2-BTMA]; Martina F. Ferracane, *The Costs of Data Protectionism*, *in* BIG DATA AND GLOBAL TRADE LAW 63–82 (Mira Burri ed., 2021); Richard D. Taylor, *"Data localization": The Internet in the Balance*, 44 TELECOMM. POL'Y (2020). For an opposing opinion, see Svetlana Yakovleva & Kristina Irion, *Pitching Trade against Privacy: Reconciling EU Governance of Personal Data Flows with External Trade*, 10 INT'L DATA PRIVACY L. 201 (2020).

B. LEGAL FRAMEWORKS FOR THE PROTECTION OF PRIVACY

I. International rules for the protection of privacy

International law establishes the right to privacy, which is now commonly referred to as one of the fundamental rights to which every human being should be entitled.[47] The core privacy principle can be found in Article 12 of the Universal Declaration of Human Rights ("UDHR"),[48] and privacy rights were given formal legal protection in Article 17 of the International Covenant on Civil and Political Rights ("ICCPR").[49] Article 17 guaranteed individuals protection of their personal sphere as broadly conceived.[50] However, this protection has not been robust. Some scholars have shown, by looking at the negotiation histories of the UDHR and the ICCPR, that the right to privacy as an umbrella term almost accidentally found its way into the treaties and was only later enshrined in national constitutions.[51] Over the years, the international framework for privacy has expanded, in particular due to the effects of new technologies and the new perils they may bring to data protection.[52] Despite the fact that the Human Rights Committee has not yet developed a specific set of obligations in the domain of privacy law, it did recognize some of its core aspects, such as that personal information ought to be protected against both public authorities and private entities, the need for data security, the right of data subjects to be informed about the processing of their data, and the right to rectification or elimination of unlawfully obtained or inaccurate data.[53] In 1990, the UN General Assembly also adopted

47. *See* G.A. Res. 217 (III) A, Universal Declaration of Human Rights, art. 12 (Dec. 10, 1948).

48. *Id.* ("No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.").

49. International Covenant on Civil and Political Rights, art. 17, Dec. 16, 1966, 999 U.N.T.S 1057.

50. The text of Article 17 is identical to Article 12 of the Universal Declaration of Human Rights, but the two sentences are framed as separate paragraphs. *See id.* at art. 17; *see* GA Res. 217 (III), *supra* note 47, at art. 12.

51. *See* Oliver Diggelmann & Maria N. Cleis, *How the Right to Privacy Became a Human Right*, 14 HUM. RTS. L. REV. 441, 446–47 (2014).

52. *See, e.g.*, Organisation for Economic Co-Operation and Development [OECD], *The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines*, at 7–8, OECD Digital Economy Papers No. 176 (Apr. 6, 2011) [hereinafter *The Evolving Privacy Landscape*].

53. U.N. Human Rights Committee, General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, ¶ 10 (Apr.

Guidelines for the Regulation of Computerized Personal Data Files ("Guidelines")[54] that stipulate minimum guarantees and include certain key principles of data protection, such as lawfulness, fairness, accuracy, purpose-specification, relevance and adequacy of data collection and processing, and data security.[55] However, the Guidelines are non-binding and states may depart from the mentioned principles for reasons of national security, public order, public health or morality, and the rights of others.[56] More recently, the appointed UN Special Rapporteur on the Right to Privacy[57] discussed his efforts to develop an international legal instrument regarding surveillance and privacy;[58] yet such an instrument has still not materialized.

The Council of Europe ("CoE") has played an important role in the evolution of the international regime by endorsing stronger and enforceable standards of human rights' protection in its 47 members through the 1950 European Convention on Human Rights ("ECHR"),[59] and through case-law developed by the European Court of Human Rights ("ECtHR") on Article 8.[60] This jurisprudence not only stressed

8, 1988), https://www.refworld.org/docid/453883f922.html [https://perma.cc/9ZEE-JNJN].

54. *See generally* G.A. Res. 45/95 (Dec. 14, 1990).

55. *See id.*

56. *See id.* ¶ 6.

57. The Special Rapporteur is an independent expert appointed by the Human Rights Council to examine and report back on a country situation and on the specific right to privacy. In July 2015, the Human Rights Council appointed Prof. Joseph Cannataci of Malta as the first-ever Special Rapporteur on the right to privacy. On the position and the specific mandate, see *Special Rapporteur on the Right to Privacy*, U.N. HUM. RTS. OFF. HIGH COMM'R, https://www.ohchr.org/en/issues/privacy/sr/pages/srprivacyindex.aspx [https://perma.cc/P9AT-V2P8].

58. *See* Joseph A. Cannataci, *Games People Play: Unvarnished Insights about Privacy at the Global Level*, *in* DATA PROTECTION AND PRIVACY UNDER PRESSURE 13, 13–48 (Gert Vermeulen & Eva Lievens eds., 2017).

59. The text of the ECHR and the additional protocols and their signatories are available on the European Court of Human Rights' website. *See generally European Convention on Human Rights*, EUR. CT. OF HUM. RTS https://www.echr.coe.int/Pages/home.aspx?p=basictexts&c= [https://perma.cc/HSS3-SLGF].

60. Convention for the Protection of Human Rights and Fundamental Freedoms, art. 8, Nov. 4, 1950, 213 U.N.T.S. 221 ("(1) Everyone has the right to respect for his private and family life, his home and his correspondence. (2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.").

the obligations of states to protect an individual's privacy rights, but also clarified the limitations of the right imposed either by key public interests or the rights of others.[61] Different aspects of data protection were further endorsed through a number of CoE resolutions and Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108"), which opened for signature in 1981 and was last amended in 2018.[62] Convention 108 is the first international instrument that established minimum standards for personal data protection in a legally binding manner.[63] Convention 108 is also open for accession to non-CoE members — so far, nine countries have joined and others have observer-status.[64]

II. Transnational rules for the protection of privacy: The OECD and the APEC frameworks

As mentioned previously, the OECD was the first organization to endorse principles of privacy protection by recognizing both the need to facilitate trans-border data flows as a basis for economic and social development and the related risks.[65] The 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data ("OECD Guidelines")[66] sought to achieve this balance by (1) agreeing upon certain basic principles of national and international application, which, while keeping free data flows, permitted legitimate restrictions, and (2) by offering bases for national implementation and international cooperation.[67] The OECD Guidelines endorse eight principles, applicable in both the public and the private sector, and also encourage countries to develop their own privacy protection frameworks along them.[68] These eight principles are: (1) collection limitation; (2) data

61. For a comprehensive guide to the jurisprudence, see, e.g., EURO. CT HUM. RTS., GUIDE ON ARTICLE 8 OF THE EUROPEAN CONVENTION ON HUMAN RIGHTS: RIGHT TO RESPECT FOR PRIVATE AND FAMILY LIFE, HOME AND CORRESPONDENCE 38–55 (2020).

62. *See generally* Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Jan. 28, 1981, 1496 U.N.T.S. 66.

63. *See, e.g.*, EUR. AGENCY FOR FUNDAMENTAL RTS. ET AL., HANDBOOK ON EUROPEAN DATA PROTECTION LAW 15–17 (2018).

64. Argentina, Burkina Faso, Cape Verde, Mauritius, Mexico, Morocco, Senegal, Tunisia, and Uruguay have become members. For details and updates, see *Data Protection – Convention 108 and Protocols: Parties*, COUNCIL OF EUR., https://www.coe.int/en/web/data-protection/convention108/parties [https://perma.cc/M7A9-PB44].

65. *The Evolving Privacy Landscape*, *supra* note 52, § 7.

66. OECD, *Guidelines for Protections*, *supra* note 13.

67. *Id.*

68. OECD, *Privacy Framework*, *supra* note 15.

quality; (3) purpose specification; (4) use limitation; (5) security safeguards principle; (6) openness; (7) individual participation; and (8) accountability.[69] These principles have become essential aspects to all national data protection regimes that were later developed, including the EU framework, which is discussed in more detail in the next section. In trying to keep pace with newer technological advances, the OECD Guidelines were revised in 2013,[70] but these core principles remained unaltered.[71] The revision added a number of new concepts, including: national privacy strategies; privacy management programs; and data security breach notification, which allow flexibility in implementation while recognizing the newer demands from governments to approach data protection as an ever more important topic.[72] Two features remain key to the OECD Guidelines: the focus on the practical implementation of privacy protection through an approach grounded in risk management and the need to address the global dimension of privacy through improved interoperability.[73]

The 2005 APEC Privacy Framework ("Privacy Framework")[74] is in many ways similar to the OECD Privacy Guidelines[75] because it contains a set of principles and implementation guidelines that were created to establish effective privacy protection that avoids barriers to information flows in the Asia Pacific Economic Cooperation ("APEC") region of 21 countries.[76] Building upon the Privacy Framework, APEC developed the Cross-Border Privacy Rules ("CBPR") system, which Australia, China Taipei, Canada, Japan, South Korea, Mexico, Singapore and the United States have formally joined.[77] The CBPR system does not displace a country's domestic laws, nor does it demand specific changes to them, but rather provides a minimum level of

69. *Id.*

70. *Id.*

71. OECD, *supra* note 13.

72. *See id.*

73. *Id.*

74. ASIA-PACIFIC ECONOMIC COOPERATION, APEC PRIVACY FRAMEWORK (2005).

75. The APEC framework endorses similar to the OECD Privacy Guidelines principles: (1) preventing harm; (2) notice; (3) collection limitations; (4) use of personal information; (5) choice; (6) integrity of personal information; (7) security safeguards; (8) access and correction; and (9) accountability. *See* Graham Greenleaf, *The APEC Privacy Initiative: "OECD Lite" for the Asia-Pacific?*, 71 PRIV. L. & BUS. 16, 16–18 (2004).

76. *See* ASIA-PACIFIC ECONOMIC COOPERATION, APEC PRIVACY FRAMEWORK ¶ 4 (2005).

77. *See About CBPRs*, CROSS BORDER PRIVACY RULES SYSTEM, http://cbprs.org/about-cbprs/ [https://perma.cc/NF9Z-GBNX].

protection through certain compliance and certification mechanisms.[78] It requires that participating businesses develop and implement data privacy policies that are consistent with the APEC Privacy Framework.[79] The APEC Accountability Agents can then assess this consistency.[80] The CBPR system is, in this sense, analogous to the EU-US Privacy Shield, which we discuss later, because they both provide a means for self-assessment, compliance review, recognition, dispute resolution, and enforcement.[81] While both the OECD and APEC privacy frameworks are non-binding,[82] they illustrate the need for international cooperation in the field of data protection, as well as the importance of cross-border data flows as a foundation of contemporary economies.

III. National approaches for data protection: The European Union versus the United States

1. Data protection in the European Union

The EU subscribes to a rights-based, omnibus data protection.[83] The right to privacy is a key concept in EU law that lawmakers have given significant weight that reflects deep cultural values and understandings. Building upon the Council of Europe's ECHR, which protects the right to private and family life,[84] the Charter of

78. Alex Wall, *International Association of Privacy Professionals, GDPR Matchup: The APEC Privacy Framework and Cross-Border Privacy Rules*, INT'L ASS'N PRIVACY PRO. (May 31, 2017), https://iapp.org/news/a/gdpr-matchup-the-apec-privacy-framework-and-cross-border-privacy-rules/# [https://perma.cc/XXE9-5A4D].

79. *Id.*

80. *See id.*

81. *See* Nigel Waters, *The APEC Asia-Pacific Privacy Initiative: A New Route to Effective Data Protection or a Trojan Horse for Self-Regulation*, 6 SCRIPTED 74, 74–89 (2009).

82. *See* OECD, *supra* note 15; *Cover Your Assets: APEC'S Privacy Framework*, ASIA-PACIFIC ECONOMIC COOPERATION (Apr. 17, 2009), https://www.apec.org/Press/Features/2009/0417_privacy [https://perma.cc/6482-KBV4]. Some scholars have argued that such soft law frameworks are nonetheless far-reaching, as their implementation depends on the power of reputational constraints as treaties do. *See, e.g.*, Chris Brummer, *How International Financial Law Works (and How It Doesn't)*, 99 GEO. L.J. 257, 263–72 (2011).

83. *See, e.g.*, Christopher F. Mondschein & Cosimo Monda, *The EU's General Data Protection Regulation (GDPR) in a Research Context*, *in* FUNDAMENTALS OF CLINICAL DATA SCIENCE 55, 57 (Peter Kubben et al. eds. 2019).

84. European Convention on Human Rights art. 8, Nov. 4, 1950, 213 U.N.T.S. 221.

Fundamental Rights of the European Union ("CFREU")[85] distinguishes between the right of respect for private and family life in Article 7 and the right to protection of personal data in Article 8.[86] This distinction is no coincidence but reflects the heightened concern of the EU and translates into a positive duty[87] to implement an effective system to protect personal data and regulate the transmission of such data.[88] The 1995 Data Protection Directive ("Directive") formed an important part of this ongoing project of the EU.[89] As the regulatory environment profoundly changed, the use and role of data in the economy demanded an update to ensure the needed high level protection of privacy. The Treaty of Lisbon, which entered into force in 2009,[90] also prompted the more active involvement of the EU as a supranational unity.[91] Next to this broad underlying need to modernize existing rules and make them fit for the new digital space, there were a number of more concrete decisions and events that triggered the change, as well as made it politically feasible. An important, albeit not directly related, development was the revelations made in 2013 by Edward Snowden that exposed the breadth and depth of surveillance by the US National

85. Charter of Fundamental Rights of the European Union, 2010 O.J. (C 83) 389.

86. *Id.* at art. 8 ("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.").

87. *See generally* Refah Partisi (The Welfare Party) and Others v. Turkey, App Nos. 41340/98, 41342/98, 41343/98 and 41344/98 (Feb. 13, 2003). *See also* Juliane Kokott & Christoph Sobotta, *The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR*, 3 INT'L DATA PRIVACY L. 222, 223–26 (2013).

88. *See id.* at 223–24.

89. 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 O.J. (L 281) 31, 31–50.

90. Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community art. 2, Dec. 13, 2007, 2007 O.J. (C 306) 1.

91. *See* Christoher Kuner, *The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law*, BLOOMBERG BNA PRIVACY AND SECURITY LAW REPORT 1–15 (2012); ORLA LYNSKEY, THE FOUNDATIONS OF EU DATA PROTECTION LAW (2015); *see also Shaping the EU as We Know it: The First 10 Years of the Lisbon Treaty 2000-2010*, COUNCIL OF THE EUR. UNION, https://www.consilium.europa.eu/en/lisbon-treaty/ [https://perma.cc/EM8T-NAQN].

Security Agency ("NSA").[92] This involved the surveillance's access to the data of millions of private users, from the systems of Google, Facebook, Apple and other big (US-based) Internet players.[93] Additionally, a series of seminal decisions of the CJEU brought about important changes in existing legal practices, as well as in the overall understanding of an individual's rights to be protected on the Internet in Europe — *Google Spain*, as previously mentioned,[94] is perhaps the best known in this context, as it coined "the right to be forgotten," which gave priority to privacy over free speech rights and the economic rights of the information intermediaries, such as Google search.[95] Another important case was *Schrems I*, decided on October 6, 2015,[96] which rendered the Safe Harbor Agreement between the EU and the US invalid and illuminated the importance of cross-border data flows, as well as the difficulties with reconciling it with the fundamental right to privacy.[97]

The new EU data protection act, the 2018 GDPR, serves the same purpose as the 1995 Data Protection Directive and seeks to harmonize the protection of fundamental rights and freedoms of natural persons regarding processing activities and to ensure the free flow of personal data between EU Member States.[98] The GDPR endorses a clear set of principles[99] and particularly high standards of protection in the form of

92. *See* Ian Brown & Douwe Korff, *Foreign Surveillance: Law and Practice in a Global Digital Environment*, 3 EURO. HUM. RTS. L. REV. 243–51 (2014).

93. *See, e.g.*, *id.* at 243–51.

94. Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, ECLI:EU:C:2014:317 (May 13, 2014).

95. *Id.* ¶ 20(3). *See also* Case C-136/17, GC and Others, EU:C:2019:773 (Sept. 24, 2019); Case C-507/17, Google v. CNIL, EU:C:2019:772 (Sept. 24, 2019); for a commentary, see, e.g., Jure Globocnick, *The Right to be Forgotten is Taking Shape: CJEU Judgments in GC and Others (C-136/17) and Google v. CNIL (C-507/17)*, 69 GRUR INT'L 380, 380–388 (2020).

96. Case C-362/14, Maximillian Schrems v. Data Prot. Comm'r, ECLI:EU:C:2015:650 (Oct. 6, 2015).

97. *See id.*

98. GDPR, *supra* note 31, at art. 3.

99. Article 5 of the GDPR specifies that personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject (*principle of lawfulness, fairness and transparency*); collected for specified, explicit and legitimate purposes (*principle of purpose limitation*); processing must also be adequate, relevant and limited to what is necessary (*principle of data minimization*); as well as accurate and, where necessary, kept up to date (*principle of accuracy*); data is to be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed

enhanced user rights (such as the already mentioned right to be forgotten,[100] the right to transparent information,[101] the right of access to personal data,[102] the right to data portability,[103] the right to object,[104] and the right not to be subject to automated decision-making, including profiling).[105] The conditions of consent,[106] as an essential element for making data processing lawful,[107] have also been changed to strengthen the user's informational sovereignty. So, for instance, pursuant to Article 7 of the GDPR, the request for consent needs to be presented in a manner that is clearly distinguishable from others, is in an intelligible and easily accessible form, and uses clear and plain language.[108] Moreover, the data subject has the right to withdraw her consent at any time.[109] As the GDPR explicitly prescribes: "[i]t shall be as easy to withdraw consent as to give it."[110] Additionally, the GDPR calls for heightened responsibilities of entities controlling and processing data, including data protection by design and by default,[111] and envisages high penalties for non-compliance.[112]

(*principle of storage limitation*); data processing must be secure (*principle of integrity and confidentiality*); and the data controller is to be held responsible (*principle of accountability*). GDPR, *supra* note 31, at art. 5.

100. *Id.* at art. 17.

101. *Id.* at art. 12.

102. *Id.* at arts. 13–15, 19.

103. *Id.* at art. 20.

104. *Id.* at art. 21.

105. *Id.* at art. 22.

106. *Id.* at art. 4(11). Article 4(11) of the GDPR clarifies the concept of consent. It states, "consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her." *Id.*

107. *Id.* at art. 7. There are special conditions applicable to child's consent. The processing of personal data based on consent pursuant to Article 6 (1) is only lawful, if the child is at least 16 years old, or consent is given or authorized by the holder of parental responsibility. Member States can provide by law for a lower age, but not below thirteen. *Id.* at art. 8(1).

108. *Id.* at art. 7(2).

109. *See* European Data Protection Board [EDPB], Guidelines 05/2020 on Consent Under Regulation 2016/679, (May 4, 2020).

110. GDPR, *supra* note 31, at art. 7(3).

111. *Id.* at art. 25.

112. *See id.* at art. 83(5)–(6). Depending on the infringement, data protection authorities can impose fines up to 20,000,000 EUR, or in the case of an undertaking, up to 4% of its total worldwide annual turnover of the preceding financial year, whichever is higher, *id.*

Also noteworthy is the firmer grasp of the GDPR in terms of its territorial reach. Article 3(1) specifies the territorial scope as covering the processing of personal data in the context of the activities of an establishment of a controller or a processor in the EU, regardless of whether the processing takes place in the EU.[113] However, the GDPR applies to a controller or processor not established in the EU, when the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the EU; or (b) the monitoring of their behavior as far as their behavior takes place within the EU.[114] This is a substantial extension of the scope of EU's data protection law and is bound to have a significant impact in its implementation, potentially becoming applicable to many US and other foreign companies targeting the EU market.[115]

In the context of the extraterritorial application of the GDPR and what has been particularly controversial, as exemplified by *Schrems I* and more recently in 2020 by *Schrems II*,[116] is the possibility of the European Commission to find that a third country offers "an adequate level of data protection."[117] With this, the EU unilaterally evaluates the

113. *Id.* at art. 3(1)

114. *Id.* at art. 3(2). Guidance to determine whether a controller or a processor is offering goods or services to EU data subjects is provided in Recital 23 of the GDPR, as well as in more detail by the European Union's data protection authority, *id.* at Recital 23. *See also* European Data Protection Board [EDPB], Guidelines 03/2018 on the Territorial Scope of the GDPR (Article 3), (Nov. 12, 2019).

115. *See, e.g.*, Paul M. Schwartz, *Information Privacy in the Cloud*, 161 U. PA. L. REV. 1623 (2013); OMER TENE & CHRISTOPHER WOLF, OVEREXTENDED: JURISDICTION AND APPLICABLE LAW UNDER THE EU GENERAL DATA PROTECTION REGULATION (2013); Mira Burri & Rahel Schär, *The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy*, 6 J. INFO. POL'Y 479 (2016); Christopher Kuner, *Reality and Illusion in EU Data Transfer Regulation Post Schrems*, 18 GERMAN L. J. 881 (2017).

116. Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd., Maximillian Schrems, ECLI:EU:C:2020:559 (July 16, 2020).

117. GDPR, *supra* note 31, at art. 45(1); *see also id.* ¶¶ 103–104. The adoption of an adequacy decision involves a proposal from the European Commission; an opinion of the European Data Protection Board; an approval from representatives of EU countries; and the adoption of the decision by the European Commission. At any time, the European Parliament and the Council may request the European Commission to maintain, amend or withdraw the adequacy decision on the grounds that its act exceeds the implementing powers provided for in the regulation. *See* GDPR *supra* note 31, at arts. 45(3) & 93(2). The Commission must regularly review the adequacy decisions and, where available information reveals, that a third country no longer ensures an adequate level of protection, repeal, amend or suspend the decision. GDPR, *supra* note 31, at art. 45(5).

standards of protection in the partner country. This would mean that personal data could flow from the EU (and Norway, Liechtenstein, and Iceland, as members of the European Economic Area) to a third country without any further safeguards being necessary,[118] or in other words, transfers to the third country become assimilated to intra-EU transmissions of data. The European Commission has so far recognized Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, and Uruguay as having adequate levels of data protection, and has ongoing talks with South Korea.[119]

The adequacy test was somewhat strengthened post-*Schrems I*, and the Commission should "take into account how a particular third country respects the rule of law, access to justice as well as international human rights norms and standards and its general and sectoral law, including legislation concerning public security, defence and national security as well as public order and criminal law."[120] The first country subject to an adequacy decision after the adoption of the GDPR was Japan.[121] In a 58-page decision[122] the Commission found, by looking at both the levels of protection provided by Japanese general and sectoral data protection regulations, as well as the redress and oversight mechanisms, that the adequacy standard described in Article 45 of the GDPR, "interpreted in light of the Charter of Fundamental Rights of the European Union, in particular in the *Schrems* judgment, is met."[123]

In the absence of an "adequacy decision," a controller or processor may only transfer personal data to a third country only if they provide appropriate safeguards, and on condition that enforceable data subject

118. *See* GDPR, *supra* note 31, at art. 45(1). *See also id.* ¶ 103.

119. *Adequacy Decisions*, EUR. COMM'N, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en [https://perma.cc/3ZYR-MRNW].

120. GDPR, *supra* note 31, at art. 45(2). *See also id.* ¶ 104.

121. GDPR Brief: Japan obtains the first adequacy agreement under the GDPR, Glob. All. for Geonomics & Health (Oct. 3, 2019), https://www.ga4gh.org/news/gdpr-brief-japan-obtains-the-first-adequacy-agreement-under-the-gdpr/ [https://perma.cc/RG9A-PS2A]. Negotiations are ongoing with South Korea and many of the existing adequacy decisions are up to renewal. Negotiations are ongoing with South Korea and many of the existing adequacy decisions are up to renewal. *See, e.g.*, *Adequacy Decisions*, *supra* note 119.

122. Commission Implementing Decision (EU) 2019/419 of 23 January 2019 Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the Adequate Protection of Personal Data by Japan Under the Act on the Protection of Personal Information, 2019 O.J. (C 304) 1.

123. *Id.* ¶ 175.

rights and effective legal remedies for data subjects are available.[124] Such appropriate safeguards may be provided for by: (a) a legally binding and enforceable instrument between public authorities or bodies; (b) binding corporate rules; (c) standard data protection clauses adopted by the Commission; (d) standard data protection clauses adopted by a supervisory authority and approved by the Commission; (e) an approved code of conduct with binding and enforceable commitments; or (f) an approved certification together with binding and enforceable commitments.[125] While the GDPR brings more clarity and certainty with regard to these clauses, they are still related to higher costs and provide only a second-best option.[126] Overall, under the EU data protection regime, priority is given to privacy protection over economic rights. The EU also seeks to "export" these higher standards by either binding individual countries through the adequacy decision or applying EU law to foreign businesses that use EU citizens' data under the GDPR.[127]

2. Data protection in the United States

The US shares a fundamentally different idea of privacy protection, which is deeply rooted in its history and understood as protection of liberty.[128] The US "focuses more on restrictions, such as the Fourth Amendment, that protect citizens from information collection and use by government rather than private actors. In fact, private actors are often protected from such restrictions by the First Amendment."[129] In

124. GDPR, *supra* note 31, at art. 46(1).

125. *Id.* at art. 46(2)(e)–(f).

126. *See* Griffin Drake, *Navigating the Atlantic: Understanding EU Data Privacy Compliance Amidst A Sea of Uncertainty*, 91 S. CAL. L. REV. 163, 180–181, 193 (2017); Alec Stapp, *GDPR After One Year: Costs and Consequences,* TRUTH ON THE MARKET (May 24, 2019), https://truthonthemarket.com/2019/05/24/gdpr-after-one-year-costs-and-unintended-consequences/ [https://perma.cc/SP44-WW67].

127. *See generally* Laurent Barthelemy, *One Year On, EU's GDPR Sets Global Standard for Data Protection*, PHYS ORG (May 24, 2019), https://phys.org/news/2019-05-year-eu-gdpr-global-standard.html [https://perma.cc/9ZZW-Z83D].

128. *See, e.g.*, James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L. J. 1151; Paul M. Schwartz, *The EU-US Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. L. REV. 1966 (2013); Paul M. Schwartz & Daniel J. Solove, *Reconciling Personal Information in the United States and European Union*, 102 CAL. L. REV. 877 (2014).

129. Larry Downes, *The Business Implications of the EU-U.S. "Privacy Shield"*, HARV. BUS. REV. (Feb. 10, 2016), https://hbr.org/2016/02/the-business-implications-of-the-eu-u-s-privacy-shield [https://perma.cc/X2JV-ABKT]. The Privacy Act of 1974 (as amended, 5 U.S.C. § 552(a)), despite bearing this broad title, applies only to data

addition, policies around Internet freedom in the US have sought "to preserve and expand the Internet as an open, global space for free expression, for organizing and interaction, and for commerce."[130] This has been recently confirmed by the White House strategy on AI.[131]

Under the First Amendment, the US has given free speech robust protection while data protection is regulated in a fragmented manner through federal privacy laws and a number of state laws.[132] These laws either concern the public sector only or they are information-specific or medium-specific, for example through the regulation of health information, video privacy, or electronic communications.[133] While the Federal Trade Commission ("FTC") can adjudicate unfair or deceptive trade practices to discipline companies that fail to implement minimal data security measures or fail to meet its privacy policies, the US does not have an official data protection authority.[134] As a consequence of

processing conducted by the federal government, not by state governments or the private sector. The Privacy Act introduces a code of fair information practices that governs the collection, maintenance, use and dissemination of information about individuals that is maintained in systems of records by federal agencies. It obliges federal agencies to collect information to the greatest extent possible directly from the concerned individuals, to retain only relevant and necessary information, to maintain adequate and complete records, to provide individuals with a right of access to review and have their records corrected, and to establish safeguards to ensure the security of the information. *See, e.g.*, Schwartz & Solove (2014), *supra* note 128.

130. RICHARD A. CLARKE ET AL., THE NSA REPORT: LIBERTY AND SECURITY IN A CHANGING WORLD 158 (2014).

131. *See* THE WHITE HOUSE, GUIDANCE FOR REGULATION OF ARTIFICIAL INTELLIGENCE APPLICATIONS (2019) ("[A]gencies should continue to promote advancements in technology and innovation, while protecting American technology, economic and national security, privacy, civil liberties, and other American values, including the principles of freedom, human rights, the rule of law, and respect for intellectual property.").

132. *See, e.g.*, Ioanna Tourkochoriti, *Speech, Privacy and Dignity in France and in the U.S.A.: A Comparative Analysis*, 38 LOY. L.A. INT'L & COMPAR. L. REV. 101, 101–182 (2016) (describing the United States and its long-standing focus on freedom of expression in contrast to the evolution of privacy laws).

133. *See, e.g.*, *id.*

134. *See USA: Data Protection Laws and Regulations 2020*, ICLG (June 7, 2020), https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa [https://perma.cc/58VK-3FHL]; for a great overview of US privacy laws, see Sherri J. Deckelboim, *Consumer Privacy on an International Scale: Conflicting Viewpoints Underlying The EU-U.S. Privacy Shield Framework and How the Framework Will Impact Privacy Advocates, National Security, and Businesses*, 48 GEO. J. INT'L L. 263 (2017); *see also* CHRIS J. HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY (2016) (following the evolution of the F.T.C. and the growth of its regulatory reach).

this fragmentation, there is no coherent definition of personal data or sensitive personal data. There are no restrictions on the transfer of personal data by private entities; instead, self-regulation and best practices are the common model of privacy protection.[135] Additionally, data is seen as a transaction commodity and there are no limitations on data exports to other countries.[136] Overall, there is a clear tendency towards liberal, market-based governance in contrast to the socially protective, rights-based governance in Europe.[137] Even recent efforts at the state level to endorse stronger consumer privacy rights, such as the ones in California, show major differences compared to the EU's fundamental rights' model.[138] The divergence in these overall approaches, as well as the protection on the ground granted in the US in specific sectors, could hardly be deemed adequate under the EU standards.[139]

3. Bridging the EU–US differences: From Safe Harbor to the Privacy Shield and back to square one

Reconciling the different privacy protection regimes between the two major players in data governance has had many implications, including an effect on trade law. Transatlantic data flows are of

135. *See generally* Siona Listokin, *Industry Self-Regulation of Consumer Data Privacy and Security*, J. MARSHALL J. INFO. TECH & PRIVACY L. 15 (2015) (discussing the advantages to self-regulation and analyzing empirical data from various websites with regards to privacy).

136. *See* M. Anthony Mills, *Is Data a Traded Commodity?*, U.S. CHAMBER OF COM. FOUND. (May 21, 2014), https://www.uschamberfoundation.org/blog/post/data-traded-commodity/34423 [https://perma.cc/6A65-R4DV]; DATA PROTECTION REGULATIONS AND INTERNATIONAL FLOW OF DATA: IMPLICATIONS FOR TRADE AND DEVELOPMENT, UNITED NATIONS CONF. TRADE DEV. 13 (2016).

137. *See* Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 STAN. L. REV. 1315, 1347 (2000).

138. Anupam Chander, Margot E. Kaminski & William McGeveran, *Catalyzing Privacy Law*, GEO. L. FAC. PUB'N OTHER WORKS (2019); Fernanda G. Nicola & Oreste Pollicino, *The Balkanization of Data Privacy Regulation*, 123 W. VA. L. REV. 61 (2020); For a different opinion pointing towards convergence of the EU and US model of privacy protection, see Erdem Büyüksagis, *Towards a Transatlantic Concept of Data Privacy*, 30 FORDHAM INTELL. PROP. MEDIA & ENT. L. J. 139 (2019).

139. *See* Shaffer, *Globalization and Social Protection*, *supra* note 9, at 26; Schwartz, *supra* note 128, at 1980; Nicola & Pollicino, *supra* note 138; Bilyana Petkova, *Privacy as Europe's First Amendment*, 25 EUR. L. J. 140 (2019). For a different perspective, see KENNETH A. BAMBERGER & DEIRDRE K. MULLIGAN, PRIVACY ON THE GROUND: DRIVING CORPORATE BEHAVIOR IN THE UNITED STATES AND EUROPE (2015) (taking the perspective on privacy law enhancement by encouraging leadership of corporations to make strides protecting individual privacy).

economic significance for both partners,[140] so the stakes for finding a workable solution are high. This has led to an intense politization of the topic and to the creation of an ingenious set of legal mechanisms that permit transatlantic data transfers while providing certain safeguards.[141] However, these hybrid mechanisms have been under substantial pressure, both politically and judicially, and thus have been adjusted over time. The first mechanism put in place under the 1995 Directive was the so-called "Safe Harbor" scheme,[142] which contained a series of principles concerning the protection of personal data that US undertakings subscribe to on a voluntary basis.[143] However, the CJEU found in *Schrems I* that the Safe Harbor scheme did not provide an adequate level of protection of fundamental rights equivalent to that guaranteed within the EU.[144] The Court observed that the Safe Harbor scheme is applicable solely to US undertakings that adhere to it, yet it does not bind US public authorities.[145] It was also apparent that US national security, public interest, and law enforcement requirements prevailed over the Safe Harbor, meaning that US undertakings can disregard, without limitation, the rules laid down by that scheme where they conflict with such requirements[146] — thus affecting fundamental rights of EU citizens. The Court found, furthermore, that US legislation is not limited to what is strictly necessary as it permits, on a generalized basis, storage of all the personal data of all the people whose data is transferred from the EU to the US without any differentiation, limitation, or exception without an objective criterion for determining the limits of the access of the public authorities to the data and of its subsequent use.[147] Additionally, there were no legal remedies provided,[148] so the Court ultimately declared the Safe Harbor decision invalid.[149]

140. MARTIN A. WEISS & KRISTIN ARCHICK, CONG. RSCH. SERV., U.S.-EU DATA PRIVACY: FROM SAFE HARBOR TO PRIVACY SHIELD 4 (2016).

141. *See generally* Bilyana Petkova, *Privacy as Europe's First Amendment*, 25 EUR. L. J., 140, 152 (2019).

142. Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbor privacy principles and related frequently asked questions issued by the US Department of Commerce, 2000 O.J. (L 215) 7.

143. MARTIN A. WEISS & KRISTIN ARCHICK, *supra* note 140, at 5.

144. Case C-362/14, Maximillian Schrems v. Data Prot. Comm'r, ECLI:EU:C:2015:650, ¶ 97 (Oct. 6, 2015).

145. *Id.* ¶ 82.

146. *Id.* ¶ 86.

147. *Id.* ¶ 93.

148. *Id.* ¶ 95.

149. *Id.* ¶¶ 105–6.

After intense negotiations, the Safe Harbor was subsequently replaced by the so-called EU-US Privacy Shield ("Privacy Shield").[150] The Privacy Shield was more stringent and detailed than the Safe Harbor agreement. While US companies (both data controllers and processors) still self-certify on an annual basis,[151] the new arrangement provided stronger obligations for US companies to protect the personal data of European citizens according to a set of clearly defined principles.[152] In addition, there were stronger monitoring and enforcement mechanisms.[153] Organizations could choose independent recourse mechanisms in either the EU or in the US, including the possibility to voluntarily cooperate with the EU data protection authorities ("DPAs").[154] Where organizations processed human resources data, the cooperation with the DPAs was mandatory.[155] Other recourse options included independent Alternative Dispute Resolution or private-sector developed privacy programs that committed to the Privacy Principles.[156] The purpose of the Privacy Shield framework was to provide data subjects with a number of possibilities to enforce their rights, lodge complaints regarding non-compliance by US companies, and to ultimately have their complaints resolved.[157] This was not mere lip service; instead, US domestic law changed through the Judicial Redress Act of 2015,[158] which extended certain rights of judicial redress established under the Privacy Act of 1974 to EU citizens.[159] Next to the enhanced individual safeguard mechanisms, there was for the first time explicit assurance from the US that any access of public authorities to personal data will be subject to clear limitations, safeguards, and

150. Commission Implementing Decision 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, 2016 O.J. (C 4176) [hereinafter Commission Implementing Decision]. For an overview, see European Commission MEMO/16/434, EU-US Privacy Shield: Frequently Asked Questions (Feb. 29, 2016).

151. Commission Implementing Decision, *supra* note 150, ¶ 14.

152. *Id.* ¶¶ 19–29 (referring to the Notice Principle, Data Integrity and Purpose Limitation Principle, Choice Principle, Security Principle, Access Principle, Recourse, Enforcement and Liability Principle, and Accountability for Onward Transfer Principle). The principles are additionally detailed in Annex II attached to the Commission's implementing decision, *see generally id.*

153. *Id.* ¶ 8.

154. *Id.* ¶ 40.

155. *Id.*

156. *Id.*

157. *Id.* ¶¶ 43–63.

158. 5 U.S.C. § 552a.

159. *Id.*

oversight mechanisms.[160] US authorities affirmed absence of indiscriminate or mass surveillance.[161] Additionally, there was a new redress possibility through the EU-US Privacy Shield Ombudsperson, who had to be independent from the US Intelligence Community and could address individual complaints.[162] In the European Commission's assessment, all of these changes conformed with the standards set out in *Schrems I*, according to which legislation involving interference with the fundamental rights guaranteed by Articles 7 and 8 of the CFREU must impose "minimum safeguards," cannot involve "on a generalised basis, storage of all the personal data of all the persons whose data has been transferred from the European Union to the United States," and must provide sufficient legal remedies.[163]

Despite these additional safeguards and surviving three reviews of the European Commission,[164] *Schrems II*[165] still invalidated the EU-US Privacy Shield.[166] Particularly, the Court found serious risks for the rights of EU citizens due to the still persistent primacy of US law enforcement requirements over those of the Privacy Shield;[167] the lack of necessary limitations on the power of the US authorities, especially in light of proportionality requirements;[168] and the lack of remedies for EU data subjects,[169] including deficiencies in the ombudsman mechanism.[170] The *Schrems II* holding had an immediate effect — US and EU authorities are back at the negotiation table and trying to find

160. European Commission MEMO/16/2462, EU-US Privacy Shield: Frequently Asked Questions (July 12, 2016).

161. Commission Implementing Decision, *supra* note 150, ¶¶ 64–90.

162. *Id.* ¶¶ 119–122. For a great analysis of the EU-US Privacy Shield, see generally Deckelboim, *supra* note 134.

163. Commission Implementing Decision, *supra* note 150, ¶¶ 90, 124 (citing Case C-362/14, Maximillian Schrems v. Data Prot. Comm'r, ECLI:EU:C:2015:650 (Oct. 6, 2015)).

164. *See, e.g.*, *Report on the Third Annual Review of the Functioning of the EU-U.S. Privacy Shield*, COM (2019) 495 final (Oct. 12, 2019). The reviews were however constantly accompanied by critique, voiced amongst others by the European Data Protection Board (EDPB). *See, e.g.*, *EDPB, EU–U.S. Privacy Shield - Third Annual Joint Review* (Nov. 12, 2019), https://edpb.europa.eu/sites/edpb/files/files/file1/edpbprivacyshield3rdannualreport.pdf_en.pdf [https://perma.cc/WQ3P-F4FY].

165. Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd., Maximillian Schrems, ECLI:EU:C:2020:559 (July 16, 2020).

166. *Id.* ¶ 65.

167. *Id.* ¶ 164.

168. *Id.* ¶¶ 168–185.

169. *Id.* ¶¶ 191–192.

170. *Id.* ¶¶ 193–197.

a swift solution, now dubbed "an enhanced EU-US Privacy Shield"[171] or "Privacy Shield 2.0." Until such a solution materializes, which may demand various changes in US law,[172] the standard contractual clauses ("SCCs") remain the common way to allow transatlantic data transfers.[173] While the SCCs survived *Schrems II*, their implementation has become somewhat more difficult. As the CJEU underlined,

> [s]ince by their inherently contractual nature standard data protection clauses cannot bind the public authorities of third countries' but the GDPR interpreted in light of the Charter of Fundamental Rights . . . require[s] that the level of protection of natural persons guaranteed by that regulation is not undermined, it may prove necessary to supplement the guarantees contained in those standard data protection clauses.[174]

The assessment of whether the countries to which data are sent offer adequate protection is primarily the responsibility of the exporter and the importer when considering whether to enter into SCCs.[175] When performing this prior assessment, the exporter must take into consideration the content of the SCCs, the specific circumstances of the transfer, and the legal regime applicable in the importer's country.[176] If the result of this assessment is that the country of the importer does not provide an equivalent level of protection, the exporter may consider

171. *See Joint Press Statement from European Commissioner for Justice Didier Reynders and U.S. Secretary of Commerce Wilbur Ross*, EUROPEAN COMMISSION (Aug. 10, 2020), https://ec.europa.eu/info/news/joint-press-statement-european-commissioner-justice-didier-reynders-and-us-secretary-commerce-wilbur-ross-7-august-2020-2020-aug-07_en [https://perma.cc/7BDD-SLSA]; *see also* CONG. RSCH. SERV., EU DATA TRANSFER REQUIREMENTS AND U.S. INTELLIGENCE LAWS: UNDERSTANDING SCHREMS II AND ITS IMPACT ON THE EU-U.S. PRIVACY SHIELD (2021).

172. *Id.*

173. Jennifer Daskal, *What Comes Next: The Aftermath of European Court's Blow to Transatlantic Data Transfers,* JUST SECURITY (July 17, 2020), https://www.justsecurity.org/71485/what-comes-next-the-aftermath-of-european-courts-blow-to-transatlantic-data-transfers/ [https://perma.cc/CT9P-8PAG].

174. Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd., ECLI:EU:C:2020:559, ¶ 132 (July 16, 2020).

175. *Statement on the Court of Justice of the European Union Judgment in Case C-311/18 - Data Protection Commissioner v Facebook Ireland and Maximillian Schrems*, EDPB (July 17, 2020), https://edpb.europa.eu/news/news/2020/statement-court-justice-european-union-judgment-case-c-31118-data-protection_en [https://perma.cc/5ZNF-HF4M].

176. *Id.*

putting additional measures in place.[177] When those contractual obligations are not or cannot be complied with, the exporter is bound by the SCCs to suspend the transfer, terminate the SCCs, or to notify its competent supervisory authority if it intends to continue transferring data.[178] Overall, the post-*Schrems II* regime places an additional burden on companies, and the absence of a proper adequacy decision substantially reduces legal certainty — which in turn puts pressure on the political actors in finding a new reconciliation mechanism. This pressure comes from private actors too and has been exemplified by the actions of the activist group "none of your business," led by Maximilian Schrems, which in the *Schrems II* aftermath filed over 100 complaints with regulators across all EU Member States against companies with European websites using code from Facebook or Google; in response the Irish Data Protection Commission sent Facebook a preliminary order to suspend data transfers to the US.[179] On the other side, Facebook has threatened withdrawal from the EU market and highlighted the grave implications for innovation and smaller businesses.[180]

177. In this regard, it is expected that the EDPB as well as national data protection authorities will provide more concrete guidelines. Such guidelines have already been made available for instance by the Data Protection Authority of German Region of Baden-Württemberg (Landesbeauftragter für Datenschutz und Informationssicherheit, LfDI). The LfDI instructs in particular the following: (1) If a data exporter intends to continue to base data transfers from the EU/EEA to the USA on the SCCs, it must create additional guarantees that prevent access by US authorities (e.g. secret services), namely through encryption, anonymization or pseudonymization of the personal data in question, and only it may have the key for re-identification; (2) Transfers to other third countries are also only permitted after prior checking of the local legal situation (existing access options by the local authorities, additional measures); (3) If the measures mentioned cannot guarantee an adequate level of protection, a transfer according to 49 GDPR is only possible according to the wording in exceptional cases and only in individual cases, for example with the consent of the persons concerned, in the context of a contract or for the assertion of legal claims. *Orientierungshilfe: Was jetzt in Sachen internationaler Datentransfer?*, LFDI (Aug. 25, 2020), https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/08/LfDI-BW-Orientierungshilfe-zu-Schrems-II.pdf [https://perma.cc/KY5J-FQN6].

178. Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd., ECLI:EU:C:2020:559, ¶¶ 133–39 (July 16, 2020); *see also Statement on the Court of Justice*, *supra* note 175.

179. *See, e.g.*, Sam Schechner & Emily Glazer, *Ireland to Order Facebook to Stop Sending User Data to U.S.*, WALL ST. J. (Sept. 9, 2020).

180. Schechner & Glazer, *supra* note 179; *see also* Alex Hern, *Facebook Says It May Quit Europe over Ban on Sharing Data with US*, THE GUARDIAN (Sept. 22, 2020).

The next sections look at the body of international trade law and mechanisms that reconcile data flows and privacy protection, starting with the rules of the WTO and continuing with the newer arrangements found in free trade agreements ("FTAs").

C. PRIVACY UNDER THE WTO FRAMEWORK

As noted above, privacy and data protection have not been a negotiation topic during the Uruguay round; the WTO law has not, as of the date of this writing, undergone any changes that reflect their growing importance or digital transformation in general.[181] Despite this, and although WTO law represents a "hard" form of international law, it does include certain mechanisms meant to reconcile economic and non-economic interests, international commitments, and domestic values and sensitivities.[182] Key amongst these mechanisms are the "general exceptions" formulated under Article XX of the General Agreement on Tariffs and Trade of 1994 ("GATT")[183] and Article XIV of the General Agreement on Trade in Services ("GATS").[184] These articles permit WTO Members to adopt measures, which would otherwise violate their obligations, under the condition that these measures are not disguised restrictions on trade.[185] Particularly interesting for this article's discussion is the possibility that Article XIV of the GATS may allow for both the existing data restrictions to remain and adoption of new data restrictions based on grounds of privacy protection. This article does not discuss the flexibilities available under the GATS, which permits WTO Members to tailor their commitments

181. *See generally* Mira Burri, *The International Economic Law Framework for Digital Trade*, 135 ZEITSCHRIFT FÜR SCHWEIZERISCHES RECHT 10 (2015); *World Trade Report 2018: The Future of World Trade: How Digital Technologies are Transforming Global Commerce*, WORLD TRADE ORG. (2018), https://www.wto.org/english/res_e/publications_e/world_trade_report18_e.pdf [https://perma.cc/7RMH-DRFD].

182. Mira Burri, *The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation*, 51 U.C. DAVIS L. REV. 65, 87–88 (2017).

183. General Agreement on Tariffs and Trade, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1A, 1867 U.N.T.S. 187 [hereinafter GATT 1994].

184. General Agreement on Trade in Services, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1B, 1869 U.N.T.S. 183 [hereinafter GATS].

185. GATT 1994, *supra* note 183; GATS, *supra* note 184.

in the different service sectors, retain substantial policy space, and maintain and adopt certain restrictive measures.[186]

While Article XIV of the GATS enumerates different grounds as possible justifications, such as the protection of human, animal, or plant life or health,[187] especially pertinent for us are two categories: (1) those relating to public order or public morals[188] and (2) those that are necessary to secure compliance with laws or regulations.[189] In the latter context, it is spelled out that this may be the case when it is necessary to secure compliance with laws or regulations relating to "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."[190] The focus here is on this provision and, for the sake of revealing how it is relevant for data flows, it is assumed that the rules of the EU GDPR are tested under it, because they were found to either violate the market access or the national treatment obligations of the EU under the GATS.[191]

Article XIV of the GATS, similarly to Article XX of the GATT, involves a number of legal tests, as established by the WTO jurisprudence: (1) the panels and the Appellate Body consider whether

186. The GATS, similarly to the GATT, is aimed at protecting equality of competitive opportunities for companies in domestic markets, regardless of their origin and the origin of their services, and at facilitating the progressive liberalization of these markets. The approach and structure of the GATS, however, differ from those of the GATT, and permit through the schedules of specific commitments "opting in" for market access and national treatment commitments. The commitments vary across sectors with very high level of liberalization for instance for telecommunication services and very low for other sectors, such as audiovisual services. *See generally, e.g.*, Pierre Sauve & Anirudh Shingal, *Reflections on the Nature of Preferences in Services*, 45 J. WORLD TRADE 953 (2011). For the level of commitments in sectors relevant for digital trade, see Burri, *supra* note 181.

187. GATS, *supra* note 184, at art. XIV(b).

188. GATS, *supra* note 184, at art. XIV(a); *see generally* Mark Wu, *Free Trade and the Protection of Public Morals: An Analysis of the Newly Emerging Public Morals Clause Doctrine*, 33 YALE J. OF INT. L. 215 (2008); Panagiotis Delimatsis, *The Puzzling Interaction of Trade and Public Morals in the Digital Era*, *in* TRADE GOVERNANCE IN THE DIGITAL AGE 276, 276–296 (Mira Burri & Thomas Cottier eds., 2012).

189. GATS, *supra* note 184, at art. XIV(c). For a commentary of Article XIV GATS, see Thomas Cottier, Panagiotis Delimatsis & Nicolas Diebold, *Article XIV GATS: General Exceptions*, *in* 6 MAX PLANCK COMMENTARIES ON WORLD TRADE LAW: TRADE IN SERVICES 287, 287–328 (Rüdiger Wolfrum et al. eds., 2008).

190. GATS, *supra* note 184, at art. XIV(c)(ii).

191. For a fully-fledged analysis of how this may occur, see Rolf H. Weber, *Regulatory Autonomy and Privacy Standards Under the GATS*, 7 ASIAN J. WTO & INT'L HEALTH L. & POL'Y 25 (2012); KRISTINA IRION ET AL., TRADE AND PRIVACY: COMPLICATED BEDFELLOWS? 27–33 (2016).

the measure falls within the scope of one of the listed objectives in the exception;[192] (2) the measure must address the relevant public interest at issue, with a sufficient nexus between the measure and the objective pursued;[193] and (3) the measure is examined under the chapeau (the introductory paragraph) of Article XIV of the GATS.[194] With regard to (1), there has been a wide margin of appreciation given to a WTO Member in the choice of objectives it seeks to protect.[195] Further, (2) is much more complex and triggers the so-called "necessity" test. The Appellate Body noted that there are different degrees of necessity.[196] At one end of this continuum lies "necessary," which is understood as "indispensable," while at the opposite side, "necessary" is taken to mean "making a contribution to."[197] The Appellate Body noted that a "necessary" measure is located significantly closer to the pole of "indispensable" than to simply "making a contribution to."[198] The more important the interest that the measure is designed to protect and the greater the contribution to the objective, the easier it is to accept the measure as "necessary."[199] However, the Appellate Body has also stated that the requirement for measures "relating to" a goal (as is the case with the GATS privacy exception), is "more flexible textually" than a strict "necessity" requirement and may simply require a "substantial" or "reasonable" relationship of the measure to the objective pursued.[200]

192. Appellate Body Report, *United States—Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, ¶ 292, WTO Doc. WT/DS285/AB/R (Apr. 7, 2005) [hereinafter *US—Gambling*].

193. *Id.*; *see also* WTO Appellate Body Report, *Brazil—Measures Affecting Imports of Retreaded Tyres*, WT/DS332/AB/R (Dec. 3, 2007), ¶¶ 119–124.

194. *US—Gambling, supra* note 192, ¶ 292.

195. *Id.* ¶ 304.

196. Appellate Body Report, *Korea—Measures Affecting Imports of Fresh, Chilled and Frozen Beef*, ¶ 161, WTO Doc. WT/DS161/AB/R, WT/DS169/AB/R (Dec. 11, 2000) [hereinafter *Korea—Beef*].

197. *Id.*

198. *Korea—Beef*, *supra* note 196.

199. *US—Gambling*, *supra* note 192, ¶¶ 306–307; *see also* Panel Report, *Argentina—Measures Relating to Trade in Goods and Services*, ¶¶ 7.680, 7.685, WTO Doc. WT/DS453/R (Sept. 30, 2015) [hereinafter *Argentina—Financial Services*] (referring to *Korea—Beef*, *supra* note 196, ¶¶ 162–163).

200. *Korea—Beef*, *supra* note 196, n.104 (citing Appellate Body Report, *United States—Standards for Reformulated and Conventional Gasoline,* ¶ 19, WTO Doc. WT/DS2/AB/R (Apr. 9, 1996); *see also* Appellate Body Report, *United States—Import Prohibition of Certain Shrimp and Shrimp Products,* ¶ 141, WTO Doc. WT/DS58/AB/R (Oct. 12, 1998).

Ultimately, WTO panels and the Appellate Body have clarified that this "weighing and balancing"[201] of factors should also include a comparison of the challenged measure and its possible alternatives.[202] To show that the measure does not meet the necessity test, a claimant can demonstrate that a less trade-restrictive alternative to the measure has been "reasonably available."[203] The alternative measure cannot pose prohibitive costs or substantial technical difficulties to implement.[204] A measure that has been provisionally justified under these material requirements of Article XIV(c)(ii) of the GATS must also meet the chapeau test, which states that a measure should not be applied in a manner that would constitute a means of arbitrary or unjustifiable discrimination between countries where like-conditions prevail, or is a disguised restriction on trade in services.[205] The chapeau has been interpreted as preventing abuses or misuses of the right to invoke the exception[206] and evaluating the "consistency of enforcement" of the challenged measure.[207]

Admittedly, these tests set a high hurdle for WTO Members, and the "success rate" for passing through them has been rather low.[208] Scholars have argued that if the EU would be challenged before a WTO panel, its GDPR may also fail to satisfy this test on several particular grounds.[209] Irion and others have argued that the EU may face a

201. *See US—Gambling, supra* note 192, ¶ 78; *see also* Appellate Body Report, *China—Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products*, T/DS363/AB/R, ¶ 239 (Dec. 21, 2009) [hereinafter *China—Publications and Audiovisual Products*].

202. *US—Gambling, supra* note 192, ¶ 306; *Argentina—Financial Services, supra* note 199, ¶ 7.684.

203. *Korea—Beef*, *supra* note 196, ¶ 166.

204. *US—Gambling, supra* note 192, ¶ 308. This case was cited with approval in *Argentina—Financial Services, supra* note 199, ¶ 7.729.

205. *US—Gambling, supra* note 192, ¶ 339.

206. *Argentina—Financial Services*, *supra* note 199, ¶ 7.743.

207. In *US—Gambling*, the Appellate Body confirmed that the US ban on online gambling did not meet the requirement of the chapeau of Article XIV GATS due to ambiguity in relation to the scope of one US statute, which appeared to permit domestic suppliers to have remote betting services for horse racing. *US—Gambling, supra* note 192, ¶ 351.

208. Only one case has so far passed all the tests. *See* Appellate Body Report, *US—Import Prohibitions of Certain Shrimp and Shrimp Products*, ¶ 186, WTO Doc. WT/DS58/AB/RW (Oct. 22, 2001); *see also* Robert Howse, *The Appellate Body Rulings in the Shrimp/Turtle Case: A New Legal Baseline for the Trade and Environment Debate*, 27 COLUM. J. ENV'T L. 489, 492 (2002).

209. Joshua D. Blume, *Reading the Trade Tea Leaves: A Comparative Analysis of Potential United States WTO-GATS Claims Against Privacy,*

problem with finding appropriate evidence on the performance of its data protection law.[210] For instance, the EU-US Safe Harbor,[211] as now invalidated,[212] was not particularly stringent as shown by *Schrems I*. One can argue that this undermines the strength of a challenged measure's contribution to securing compliance with the EU's data protection law. Second, and this is a critical argument, it can well be maintained that there are less trade restrictive measures that are reasonably available for achieving the EU's desired level of data protection. The GDPR is in many senses excessively burdensome with sizeable extraterritorial effects.[213] Especially if compared with other data protection rules around the world, it may be difficult to prove that privacy cannot be otherwise protected.[214] Even if the provisions on the transfer of personal data to third countries were to be deemed necessary to secure compliance with the GDPR, there is an argument to be made that these provisions have not been consistently implemented and would ultimately fail the chapeau test. If the EU has denied a third country's application for adequacy assessment or a request to negotiate a sectoral scheme similar to that of the US-EU Safe Harbor or the Privacy Shield, it seems that the chapeau test requirements are hard to meet. The EU may effectively discriminate between different countries in finding adequate levels of protection or when engaging in cooperation with them, so that the standards of protection would be secured in terms of substance and procedure.[215]

With regard to the application of Article XIV of the GATS to privacy protection matters, the scholarly debate is bound to continue as there is still no relevant case-law and as the importance of the topic increases. For now, it is critical to underline that the general exception clause under Article XIV of the GATS is a good example of both the flexibility of WTO law, as well as of its potential to intervene in domestic matters to discipline WTO Members and draw a line between

---

Localization, and Cybersecurity Laws, 49 GEO. J. INT'L L. 801, 842 (2018).

210. IRION ET AL., *supra* note 191, at 36–39; *see also* Diana A. MacDonald & Christine M. Streatfeild, *Personal Data Privacy and the WTO*, 36 HOUS. J. INT'L L. 625, 640–650 (2014) (examining the Korean online data privacy protection in a hypothetical WTO dispute).

211. *See* 2000 O.J. (L 215) 7.

212. Court of Justice of the European Union Press Release 117/15, The Court of Justice Declares that the Commission's US Safe Harbour Decision is Invalid (Oct. 6, 2015).

213. Adele Azzi, *The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation*, J. INTELL. PROP. INFO. TECH. & E-COM. L. 126, 127–128 (2018).

214. LEE ANDREW BYGRAVE, DATA PRIVACY LAW: AN INTERNATIONAL PERSPECTIVE 205 (2014); Yakoleva & Irion, *supra* note 46, at 202.

215. IRION ET AL., *supra* note 191, at 36–39.

licit protection and illicit protectionism. Despite the current deadlock at the WTO and the crisis of its dispute resolution system,[216] the interpretation of Articles XX of the GATT and XIV of the GATS remains of critical importance, as many free trade agreements stipulate their application *mutatis mutandis,* as discussed below.[217]

D. DEVELOPMENTS IN FREE TRADE AGREEMENTS

As legal adaptations under the umbrella of the WTO have stalled, bilateral and regional FTAs have addressed many issues of digital trade and data governance. Indeed, from the 353 FTAs agreed upon between 2000 and 2020, 188 FTAs have provisions of relevance for digital trade.[218] The US has been a legal entrepreneur in this context and played a key role by endorsing liberal rules in the implementation of its "Digital Agenda."[219] The agreements reached since 2002 with Australia, Bahrain, Chile, Morocco, Oman, Peru, Singapore, the Central American countries,[220] Panama, Colombia, South Korea, and Japan, as well the updated North American Free Trade Agreement ("NAFTA") with Canada and Mexico, all contain critical WTO-plus (going above the WTO commitments) and WTO-extra (addressing issues not covered by the WTO) provisions in the broader field of digital trade.[221] However, the emergent regulatory template on digital issues is not limited to US agreements but instead has diffused and can be found in other FTAs as well; Singapore, Australia, Japan, and Colombia have

216. *See, e.g.*, Joost Pauwelyn, *WTO Dispute Settlement Post 2019: What to Expect?*, 22 J. INT'L ECON. L. 297 (2019).

217. For instance, the 2020 Digital Economy Partnership Agreement between Chile, Singapore and New Zealand. *See Overview*, NEW ZEALAND FOREIGN AFFAIRS & TRADE, https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-in-force/digital-economy-partnership-agreement/overview/ [https://perma.cc/VVC7-YTXG].

218. Mira Burri & Rodrigo Polanco, *Digital Trade Provisions in Preferential Trade Agreements: Introducing a New Dataset,* 23 J. INT'L ECON. L. 187, 192 (2020).

219. *See generally* Sacha Wunsch-Vincent, *The Digital Trade Agenda of the US: Parallel Tracks of Bilateral, Regional and Multilateral Liberalization*, 58 AUSSENWIRTSCHAFT 7 (2003).

220. The DR-CAFTA includes Costa Rica, El Salvador, Guatemala, Honduras, Nicaragua and the Dominican Republic. *CAFTA-DR (Dominican Republic-Central America FTA)*, OFF. OF THE U.S. TRADE REPRESENTATIVE, https://ustr.gov/trade-agreements/free-trade-agreements/cafta-dr-dominican-republic-central-america-fta [https://perma.cc/R7PS-U6VQ].

221. Mira Burri, *Understanding and Shaping Trade Rules for the Digital Era, in* THE SHIFTING LANDSCAPE OF GLOBAL TRADE GOVERNANCE 73, 94 (Manfred Elsig et al. eds., 2019).

been amongst the major drivers of this diffusion.[222] This section maps the emerging regulatory landscape in particular regarding data-relevant norms.[223]

I. Overview of data-related rules in FTAs

Trade rules matter for data and data flows for at least three reasons because: (i) they regulate the cross-border flow of data by regulating trade in goods and services as well as the protection of intellectual property; (ii) they may install certain beyond-the-border-rules that demand changes in domestic regulation — for example, on intermediaries' liability; and (iii) trade law can limit the policy space that regulators have at home.[224] In addition to this generic trade law framework, the last decade has also witnessed the emergence of entirely new rules that address the regulation of data flows.[225] This section focuses on these rules in particular. In this context, it is first important to note that there is no common agreement on a definition for data flows in FTAs, despite the wide-spread rhetoric around the term and its frequent use in reports and studies.[226] However, despite the different terms used in treaty language, there seems to be a clear tendency for a broad and encompassing definition of data flows, (1) where there are bits of information (data) as part of the provision of a service or a product and (2) where this data crosses borders, although the data flows do not neatly coincide with one commercial transaction and the provision of a certain service may relate to multiple flows of data.[227] Additionally, there has thus far not been a distinction between different types of data so far — for instance, between personal and non-personal

222. *Id.*

223. This analysis is based on a dataset of all data-relevant norms in trade agreements (TAPED). *See* Burri & Polanco, *supra* note 218, at 192; *TAPED: A New Dataset on Data-related Trade Provisions*, UNIVERSITY OF LUCERNE, http://unilu.ch/taped [https://perma.cc/REG3-Q7KC].

224. Burri, *The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation*, *supra* note 182; *see also* Francesca Casalini & Javier López González, *Trade and Cross-Border Data Flows*, 11 (OECD Trade Pol'y Papers No. 220, 2019).

225. Burri, *The Governance of Data and Data Flows in Trade Agreements*: *The Pitfalls of Legal Adaptation*, *supra* note 182, at 68.

226. *See, e.g.*, Casalini & González, *supra* note 224, at 12 (describing the lack of consensus on a definition for personal data).

227. As the OECD further clarifies: "the actual flow of data reflects individual firm choices: accessing the OECD library from Paris, for instance, actually means contacting a server in the United States (the OECD uses a US-based company for its web services). Moreover, with the cloud, data can live in many places at once, with files and copies residing in servers around the world." *Trade and Cross-Border Trade Flows*, OECD (Oct. 2019), https://issuu.com/oecd.publishing/docs/trade_and_cross-border_data_flows [https://perma.cc/STF9-ZV8A].

data, personal or company data, or machine-to-machine data.[228] Yet, personal information is commonly included explicitly in the data-related provisions in FTAs,[229] where the potential clashes with domestic data protection regimes become evident.

Overall, specific data-related provisions are a relatively new phenomenon and are found primarily in dedicated e-commerce chapters of FTAs — but only in a handful of agreements.[230] These types of provisions generally refer to the cross-border flow of data and rules banning or limiting data localization requirements.[231] Provisions on data flows can also be found in chapters dealing with discrete service sectors where data is inherent to the very definition of those services — such as the telecommunications and financial services sectors.[232]

II. Rules on data flows and data localization in recent FTAs

Non-binding provisions on data flows appeared in early agreements, such as the 2000 Jordan-US FTA.[233] Yet, it is only in recent years that

228. For instance, Sen classifies data into personal data referring to data related to individuals; company data referring to data flowing between corporations; business data referring to digitized content such as software and audiovisual content; and social data referring to behavioral patterns determined using personal data. Nivedita Sen, *Understanding the Role of the WTO in International Data Flows: Taking the Liberalization or the Regulatory Autonomy Path?*, 21 J. INT'L ECON. L. 323, 343–346 (2018). Aaronson and Leblond categorize data into personal data, public data, confidential business data, machine-to-machine data and metadata, although they do not specifically define each of these terms. Susan Ariel Aaronson & Patrick Leblond, *Another Digital Divide: The Rise of Data Realms and its Implications for the WTO*, 21 J. INT'L ECON. L. 245, 250 fig.1 (2018). The OECD has also tried to break data into different categories. *See Data in the Digital Age, Policy Brief*, OECD (Mar. 2019) https://www.oecd.org/going-digital/data-in-the-digital-age.pdf [https://perma.cc/72JZ-EVWQ].

229. Mira Burri, *Data Flows and Global Trade Law*, *in* BIG DATA & GLOBAL TRADE LAW 11–41 (Mira Burri ed., 2021).

230. *Id.* Only some 30 FTAs have provisions on data flows and many of them are of soft law nature, *id.*

231. *Id.*

232. This article does not cover specific services sectors. For a more detailed analysis, see, e.g., Mira Burri, *Telecommunications and Media Services, in Preferential Trade Agreements: Path Dependences Still Matter, in* EUROPEAN YEARBOOK OF INTERNATIONAL ECONOMIC LAW: COHERENCE AND DIVERGENCE IN SERVICES TRADE LAW 169–192 (Rhea Tamara Hoffmann & Markus Krajewski eds., 2020).

233. A similar wording is used in the 2008 Canada-Peru FTA, 2010 Hong-Kong-New Zealand FTA, 2011 Korea-Peru FTA, 2011 Central America-Mexico FTA, 2013 Colombia-Costa Rica FTA, 2013 Canada-Honduras FTA, 2014 Canada-Korea FTA, and 2015 Japan-Mongolia FTA. The 2007 South Korea-US FTA was the first agreement with more concrete

these rules have been made binding and more comprehensive.[234] Particularly important in this context were the negotiations of the Trans-Pacific Partnership Agreement ("TPP")[235] between the US and eleven countries in the Pacific Rim.[236] The TPP sought to be a bold 21st century trade deal and thus aimed to move away from the brick-and-mortar WTO Agreements and reflect the new digital reality.[237] While the TPP did not eventually materialize because the Trump administration withdrew from it,[238] it gave the basis for two important treaties — (1) the Comprehensive and Progressive Agreement for Transpacific Partnership ("CPTPP")[239] between the remainder of the TPP parties; and (2) the renegotiated NAFTA, which is now referred to as the United States-Mexico-Canada Agreement ("USMCA").[240] The CPTPP's and the USMCA's electronic commerce chapters build upon the TPP and reflect the US agenda on the relevant issues evidenced by the creation of a comprehensive template for digital trade with strong rules on data flows.[241] We look in turn at these treaties.[242]

---

language on data flows, albeit in a soft law form (Korea-US FTA, Article 15.8). *See* Burri, *Data Flows and Global Trade Law*, *supra* note 229.

234. Mira Burri, *The Regulation of Data Flows Through Trade Agreements*, 48 GEO. J. INT'L L. 407, 425 (2017).

235. *The Trans-Pacific Partnership Agreement*, OFF. OF U.S. TRADE REP., https://ustr.gov/trade-agreements/free-trade-agreements/trans-pacific-partnership/tpp-full-text [https://perma.cc/9LYF-5EJA] [hereinafter TPP].

236. *See id.* at annex 2-D.

237. *See generally* John Ravenhill, *The Political Economy of the Trans-Pacific Partnership: A '21st Century' Trade Agreement?*, 22 NEW POL. ECON. 573 (2017).

238. Letter from Maria L. Pagan, Acting United States Trade Rep., to Trans-Pacific Partnership Depositary (Jan. 30, 2017).

239. *The Comprehensive and Progressive Agreement for Transpacific Partnership*, AUSTL. GOVERNMENT DEP'T OF FOREIGN AFFAIRS & TRADE [hereinafter CPTPP], https://www.dfat.gov.au/trade/agreements/in-force/cptpp/official-documents/Pages/official-documents [https://perma.cc/72HF-VLH4].

240. *See* Wolfgang Alschner & Rama Panford-Walsh, *How Much of the Transpacific Partnership is in the United-States-Mexico-Canada Agreement?* 2 (Ottawa Faculty of L., Working Paper No. 2019-28, 2019).

241. *See generally* Mira Burri, *Adapting Trade Rules for the Age of Big Data, in* TRADE IN KNOWLEDGE: ECONOMIC, LEGAL AND POLICY ASPECTS (Antony Taubman & Kayashree Watal eds., forthcoming 2021).

242. For a fully-fledged analysis, see Burri, *The Governance of Data and Data Flows in Trade Agreements*, *supra* note 182. *See also* Burri, *Data Flows and Global Trade Law*, *supra* note 229.

The CPTPP sought, for the first time, to explicitly restrict the use of data localization measures.[243] Article 14.13(2) prohibits the parties from requiring a "covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory."[244] The soft language from the US-South Korea FTA on free data flows is now also framed as a hard rule: "[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."[245] The rule has a broad scope and most of the data that is transferred over the internet is likely to be covered, although the word "for" may suggest the need for some causality between the flow of data and the business of the covered person.

Measures restricting digital flows or localization requirements under Article 14.13 of the CPTPP are permitted only if they do not amount to "arbitrary or unjustifiable discrimination or a disguised restriction on trade" and do not "impose restrictions on transfers of information greater than are required to achieve the objective."[246] These non-discriminatory conditions are similar to the test formulated by Article XIV of the GATS and Article XX of the GATT, which, as noted earlier, is meant to balance trade and non-trade interests.[247] The CPTPP test differs from the WTO norms in one significant element: while there is a list of public policy objectives in the GATT and the GATS (such as public morals or public order), the CPTPP provides no such enumeration and simply speaks of a "legitimate public policy objective."[248] This language permits more regulatory autonomy for the CPTPP signatories. However, it also may lead to abuses and overall legal uncertainty. Further, it should be noted that the ban on localization measures is somewhat softened regarding financial services and institutions.[249] An annex to the Financial Services chapter has a separate data transfer requirement, whereby certain restrictions on data flows may apply for the protection of privacy or confidentiality of

243. Burri, *Data Flows and Global Trade Law*, *supra* note 229.

244. CPTPP, *supra* note 239, at art. 14.13(2).

245. *Id.* at art. 14.11(2) (emphasis added).

246. *Id.* at art. 14.11(3).

247. *See* GATS, *supra* note 184, at art. XIV; GATT, *supra* note 183, at art. XX.

248. *See* CPTPP, *supra* note 239, at art. 14.11(3).

249. *See id.* at art. 14.1 (defining "a covered person" in Article 14.1, which is said to exclude a "financial institution" and a "cross-border financial service supplier").

individual records, or for prudential reasons.[250] Government procurement is also excluded.[251]

After the withdrawal of the US from the TPP,[252] there was some uncertainty as to the direction the US would follow in its trade deals, specifically on matters of digital trade.[253] The USMCA casts these doubts aside. The USMCA has a comprehensive electronic commerce chapter, which is now also properly titled "Digital Trade" and follows all critical lines of the CPTPP in ensuring the free flow of data through a clear ban on data localization,[254] providing a non-discrimination regime for digital products,[255] and a hard rule on free information flows.[256] The USMCA permits the pursuit of certain non-economic objectives.[257] Article 19.11 specifies, similar to the CPTPP, that parties can adopt or maintain a measure inconsistent with the free flow of data provision, if this is necessary to achieve a legitimate public policy objective, provided that the measure: (1) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and (2) does not impose restrictions on transfers of information greater than are necessary to achieve the objective.[258] The USMCA clarified further that "a measure does not meet the conditions of this paragraph if it accords different treatment to data transfers solely on the basis that they are cross-border in a manner that modifies the conditions of competition to

250. CPTPP, *supra* note 239, at art. 11 § B ("Each Party shall allow a financial institution of another Party to transfer information in electronic or other form, into and out of its territory, for data processing if such processing is required in the institution's ordinary course of business.").

251. *Id.* at art. 14.8(3).

252. Letter from Maria L. Pagan, *supra* note 238.

253. *See generally* RACHEL F. FEFER ET. AL., CONG. RESEARCH SERV., R44565, DIGITAL TRADE AND U.S. TRADE POLICY (May 21, 2019); *see also Fact Sheet: Key Barriers to Digital Trade*, U.S. TRADE REP. ARCHIVES, https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2016/march/fact-sheet-key-barriers-digital-trade [perma.cc/6QYD-8L7Y].

254. *Agreement Between the United States of America, the United Mexican States, and Canada*, OFF. OF U.S. TRADE REP. art. 19.12 [hereinafter USMCA], https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/agreement-between [https://perma.cc/X258-VB8X].

255. *Id.* at art. 19.4.

256. *Id.* at art. 19.11.

257. *See id.*; *see generally* M. ANGELES VILLARREAL & IAN F. FERGUSSON, CONG. RESEARCH SERV., R44981, THE UNITED STATES-MEXICO-CANADA AGREEMENT (USMCA) (July 27, 2020).

258. USMCA, *supra* note 254, at art. 19.11(2).

the detriment of service suppliers of another Party,"[259] which effectively connects to the necessity test under WTO law.

Subsequent treaties, such as the 2016 Chile-Uruguay FTA; the 2016 Updated Singapore-Australia FTA; the 2019 US-Japan Digital Trade Agreement ("DTA"), which also covers financial and insurance services; and the 2020 Digital Economy Partnership Agreement ("DEPA") between Chile, New Zealand, and Singapore closely follow the CPTPP template and enhance the diffusion of the rules on data flows and data localization.[260]

In contrast, the EU has been cautious when inserting rules on data in its free trade deals. However, recently the EU made a step towards such binding rules, where parties have agreed to consider commitments related to cross-border flow of information in future negotiations.[261] This type of clause is found in the 2018 EU-Japan EPA[262] and in the modernization of the trade section of the EU-Mexico Global Agreement.[263] In the latter two agreements, the parties commit to "reassess" the need for inclusion of provisions on the free flow of data into the treaty within three years of the entry into force of the agreement.[264] This signals a repositioning of the EU on the issue of data flows, as well as the EU's wish to link this commitment in due time with the high data protection standards of the GDPR,[265] as discussed in more detail below.

---

259. *Id.* at 19.11(2) n.5.

260. *Cf.* U.S.-Japan Digital Trade Agreement ("DTA"), Japan-U.S., Oct. 7, 2019, [hereinafter DTA] https://ustr.gov/sites/default/files/files/agreements/japan/Agreement_between_the_United_States_and_Japan_concerning_Digital_Trade.pdf [https://perma.cc/B7UQ-RWKL], *with* CPTPP, *supra* note 239.

261. *See, e.g.*, *id.* at art. 15.3(3); *see also Questions & Answers: EU-UK Trade and Cooperation Agreement*, EUROPEAN COMM'N (Dec. 24, 2020) [hereinafter *Q&A*], https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_2532 [perma.cc/TTT5-P66P].

262. Agreement Between the European Union and Japan for an Economic Partnership, E.U.-Japan, Feb. 1, 2019, at art. 8.81 [hereinafter EPA] https://trade.ec.europa.eu/doclib/docs/2018/august/tradoc_157228.pdf [https://perma.cc/JH8X-BQS4].

263. *See generally Modernisation of the Trade part of the EU-Mexico Global Agreement Without Prejudice*, EUR. COMM'N (Apr. 21, 2018), https://trade.ec.europa.eu/doclib/docs/2018/april/tradoc_156798.pdf [perma.cc/R9J2-A29X].

264. *Id.* at art. XX.

265. *See generally Horizontal Provisions for Cross-Border Data Flows and for Personal Data Protection in EU Trade and Investment Agreements*, EUR. COMM'N [hereinafter *Horizontal Provisions*]

III. Rules on data protection

Thus far, 91 FTAs include provisions on data protection.[266] Yet, the nature of the awarded protection varies considerably and can include both binding and non-binding provisions.[267] This is symptomatic of the different positions of the major actors and the inherent tensions between the regulatory goals of data innovation and data protection. Earlier agreements, such as the 2000 Jordan-US FTA Joint Statement on Electronic Commerce, address privacy issues in hortatory provisions.[268] Later agreements remain still in the domain of soft law, but include a variety of cooperation activities to improve the level of protection of privacy and curb obstacles to trade that requires transfers of personal data.[269] These activities include sharing information and experiences on regulations, laws and programs on data protection,[270] or the overall domestic regime for the protection of

https://trade.ec.europa.eu/doclib/docs/2018/may/tradoc_156884.pdf [perma.cc/NZD3-TEKN].

266. *See generally Regional Trade Agreement Database*, WTO, http://rtais.wto.org/UI/PublicAllRTAList.aspx [perma.cc/MPP7-HDY4]; *see also* TAPED, *supra* note 3.

267. *Cf.* EPA, *supra* note 262, at art. 8.81, with USMCA, *supra* note 254, at art. 19

268. Joint Statement on Electronic Commerce, Jordan-U.S., June 7, 2000, art. II, http://www.sice.oas.org/Trade/us-jrd/St.Ecomm.pdf [https://perma.cc/WAQ2-252S]; *see* United States (U.S.)-Jordan: Agreement Between The United States of America and the Hashemite Kingdom of Jordan on The Establishment of a Free Trade Area art. 7(3), October 24, 2000, 41 I.L.M. 63.

269. *See* DTA, *supra* note 260; *see, e.g.*, Stephen Ezell & Nigel Cory, *The Way Forward for Intellectual Property Internationally*, INFO. TECH. & INNOVATION FOUND. (Apr. 25, 2019), https://itif.org/publications/2019/04/25/way-forward-intellectual-property-internationally [perma.cc/LW76-SQ7L].

270. *See, e.g.*, *Brazil-Chile Free Trade Agreement*, GOVERNO DO BRAZ. MINISTÉRIO_DAS RELAÇÕES EXTERIORES arts. 10.8.5, 10.15(b), https://www.gov.br/mre/en/contact-us/press-area/press-releases/conclusion-of-negotiations-on-the-free-trade-agreement-between-brazil-and-chile-santiago-october-16-19-2018 [https://perma.cc/9VGL-B8DB]; *Free Trade Agreement Between Canada and The Republic of Korea*, GOV'T CAN. art. 13.7(b), https://www.international.gc.ca/trade-commerce/trade-agreements-accords-commerciaux/agr-acc/korea-coree/index.aspx?lang=eng [https://perma.cc/9M85-4923]; *Agreement Between Australia and Japan for an Economic Partnership*, AUSTL. GOV'T DEP'T FOREIGN AFF. art. 13.10.2, https://www.dfat.gov.au/trade/agreements/in-force/jaepa/Pages/japan-australia-economic-partnership-agreement [https://perma.cc/8GL4-D6DY]; *Acuerdo de Libre Comercio Chile-Colombia el cual constituye un protocolo adicional al ACE 24*, GOBIERNO DE COLOMBIA MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO art. 12.5(b),

http://www.tlc.gov.co/acuerdos/vigente/acuerdo-de-libre-comercio-chile-colombia#:~:text=El%20ACE24%20fue%20el%20primer,permita%20la%20libre%20circulaci%C3%B3n%20d [https://perma.cc/2MJ7-QL4S]; *Nicaragua-Republic of China (Taiwan) Free Trade Agreement*, MINISTRY OF ECON. AFF. R.O.C. art. 14.05(b), https://www.moea.gov.tw/MNS/english/news/News.aspx?kind=6&menu_id=176&news_id=92502 [https://perma.cc/3XSZ-45YA]; *Free Trade Agreement Between the Republic of Singapore and the Republic of Panama*, INT'L TRADE ADMIN. art. 13.4(b), https://www.trade.gov/knowledge-product/panama-trade-agreements [https://perma.cc/L2CG-25YN]; *CAFTA-DR (Dominican Republic-Central America FTA),* OFF. U.S. TRADE REP. art. 14.5(b), https://ustr.gov/trade-agreements/free-trade-agreements/cafta-dr-dominican-republic-central-america-fta [perma.cc/WBR9-LQZS]; *United States-Chile Free Trade Agreement*, OFF. U.S. TRADE REP. art. 15.5(b), https://ustr.gov/trade-agreements/free-trade-agreements/chile-fta [perma.cc/77BW-SGQX].

personal information;[271] technical assistance in the form of exchanging information and experts,[272] research, and training activities;[273] or the establishment of joint programs and projects.[274]

FTAs have also dealt with personal data protection with reference to the adoption of domestic standards. While some merely recognize the importance or the benefits of protecting personal information

---

271. *See, e.g.*, *Indonesia-Australia Comprehensive Economic Partnership Agreement*, AUSTL. GOV'T DEP'T FOREIGN AFF. art. 13.3.1(b)(i), https://www.dfat.gov.au/trade/agreements/in-force/iacepa/Pages/indonesia-australia-comprehensive-economic-partnership-agreement [https://perma.cc/E84R-A3D9]; USMCA, *supra* note 254, at art. 19.14.1(a)(i); *Peru-Australia Free Trade Agreement*, AUSTL. GOV'T DEP'T FOREIGN AFF. art. 13.14(b)(i), https://www.dfat.gov.au/trade/agreements/in-force/pafta/Pages/peru-australia-fta [https://perma.cc/N8SG-P87D]; *Sri Lanka – Singapore Free Trade Agreement (SLSFTA)*, ENTERPRISE SINGAPORE art. 9.12(c)(i), https://www.enterprisesg.gov.sg/non-financial-assistance/for-singapore-companies/free-trade-agreements/ftas/Singapore-ftas/SLSFTA#:~:text=Free%20Trade%20Agreement%20(SLSFTA)&text=SLSFTA%20covers%20tariff%20elimination%20for,issue%20in%20the%20exporting%20party [https://perma.cc/6545-E3MU]; *Turkey – Singapore Free Trade Agreement (TRSFTA)*, ENTERPRISE SINGAPORE art. 9.9(c), https://www.enterprisesg.gov.sg/non-financial-assistance/for-singapore-companies/free-trade-agreements/ftas/singapore-ftas/trsfta [https://perma.cc/E2ZK-H7V5]; *Free Trade Agreement Between the Government of the People's Republic of China and the Government of the Republic of Korea*, MINISTRY COM. PEOPLE'S REPUBLIC CHINA art. 13.5, http://fta.mofcom.gov.cn/topic/enkorea.shtml [https://perma.cc/MNZ7-PVSH]; *Colombia-Costa Rica Free Trade Agreement*, UNCTAD INVESTMENT POLICY HUB art. 16.6.2, https://investmentpolicy.unctad.org/international-investment-agreements/treaties/treaties-with-investment-provisions/3397/colombia--costa-rica-fta-2013- [https://perma.cc/EJY7-5QCJ]; *Canada-Colombia Free Trade Agreement*, GOV'T CAN. art. 1506.2, https://www.international.gc.ca/trade-commerce/trade-agreements-accords-commerciaux/agr-acc/colombia-colombie/fta-ale/background-contexte.aspx?lang=eng [https://perma.cc/97BS-PY4U].

272. *Agreement Establishing Association Between the European Community and its Member States, of the one part, and the Republic of Chile*, COUNCIL EUR. UNION art. 30, https://www.consilium.europa.eu/en/documents-publications/treaties-agreements/agreement/?id=2002086 [https://perma.cc/P7HH-ZR3W].

273. *Free Trade Agreement Between the Government of the Socialist Republic of Viet Nam and the Government of the Republic of Korea*, KCS TOTAL SOLUTION art. 10.8.1(b), https://www.customs.go.kr/engportal/cm/cntnts/cntntsView.do?mi=7309&cntntsId=2332 [https://perma.cc/PZ6M-R5UF].

274. *Agreement Establishing Association Between the European Community and its Member States, of the one part, and the Republic of Chile*, *supra* note 272.

online,[275] in several treaties parties specifically commit to adopt or maintain legislation or regulations that protects the personal data or privacy of its users.[276] Representative of this group are the CPTPP and the USMCA.[277] Yet, while Article 14.8(2) of the CPTPP requires every party to "adopt or maintain a legal framework that provides for the protection of the personal information of the users of electronic commerce,"[278] no standards or benchmarks for the legal framework have been specified, except for a general requirement that the parties "take into account principles or guidelines of relevant international bodies."[279] A footnote provides some clarification in saying that: "[f]or greater certainty, a Party may comply with the obligation in this paragraph by adopting or maintaining measures such as a comprehensive privacy, personal information or personal data protection laws, sector-specific laws covering privacy, or laws that provide for the enforcement of voluntary undertakings by enterprises relating to privacy."[280] Parties are also invited to promote compatibility between their data protection regimes by essentially treating lower standards as equivalent.[281] Overall, the goal seems to be to prioritize trade over privacy rights.

The USMCA is interesting in two aspects when compared to the CPTPP and the US's position on data protection issues. While Article 19.8 of the USMCA remains soft on prescribing domestic regimes on personal data protection, it recognizes principles and guidelines of relevant international bodies.[282] Article 19.8 states in particular that " in the development of its legal framework for the protection of personal information, each Party should take into account principles and guidelines of relevant international bodies, such as the APEC Privacy Framework and the OECD Recommendation of the Council concerning Guidelines governing the Protection of Privacy and

275. *See, e.g.*, *Indonesia-Australia Comprehensive Economic Partnership Agreement*, *supra* note 271; *Brazil-Chile Free Trade Agreement*, *supra* note 270; EPA, *supra* note 262; *Central America – Korea Free Trade Agreement*, KCS TOTAL SOLUTION art. 14.5.1, http://www.customs.go.kr/download/ftaportalkor/_down/trty/han_ma_02_eng.pdf [https://perma.cc/4XTH-RGDL]; *Canada – Honduras Free Trade Agreement*, GOV'T CAN. art. 16.2.2(e), https://www.international.gc.ca/trade-commerce/trade-agreements-accords-commerciaux/agr-acc/honduras/fta-ale/background-contexte.aspx?lang=eng [https://perma.cc/U6E7-N5GB].

276. *See* CPTPP, *supra* note 239, annex § 7(e).

277. *Id.*; USMCA, *supra* note 254, at art. 19.8.

278. CPTPP, *supra* note 239, at art. 14.8(2).

279. *Id.*

280. *Id.* at art. 14.8(2) n.6.

281. *See id.* at art. 14.8(5).

282. *See* USMCA, *supra* note 254, at art. 19.8.

Transborder Flows of Personal Data (2013)."[283] The USMCA parties also recognize key principles of data protection. These include: limitation on collection; choice; data quality; purpose specification; use limitation; security safeguards; transparency; individual participation; and accountability,[284] and aim to provide remedies for any violations.[285] This is interesting because it may go beyond what the US has in its national laws on data protection and also because it reflects some of the principles the EU has advocated in the domain of the protection of privacy. One may speculate, as discussed in more detail below, whether this is a development caused by the so-called "Brussels effect," where the EU "exports" its own domestic standards by virtue of its large domestic market and regulatory capabilities and they become global,[286] or whether we are seeing a shift in US privacy protection regimes as well.[287]

As mentioned earlier, the EU has sought more binding commitments for privacy protection in its FTAs. For instance, many of the EU's agreements have special chapters on protection of personal data, including the principles of purpose limitation, data quality and proportionality, transparency, security, right to access, rectification and opposition, restrictions on onward transfers, and protection of sensitive data, as well as provisions on enforcement mechanisms, coherence with international commitments and cooperation between the parties in order to ensure an adequate level of protection of personal data.[288] The

283. *Id.* at art. 19.8(2).

284. *Id.* at art. 19.8(3).

285. *Id.* at art. 19.8(4)–(5).

286. *See generally* Anu Bradford, *The Brussels Effect*, 107 NW. U. L. REV. 1 (2012); ANU BRADFORD, THE BRUSSELS EFFECT: HOW THE EUROPEAN UNION RULES THE WORLD (2020).

287. For a great analysis, see Chander, Kaminski & McGeveran, *supra* note 138.

288. 2009 O.J. (L 57) 61–65; *Economic Partnership Agreement between the CARIFORUM States and the European Community*, E.C., ch. 6, art. 197–201, https://trade.ec.europa.eu/access-to-markets/en/content/eu-cariforum-economic-partnership-agreement#:~:text=The%20CARIFORUM%2DEU%20Economic%20Partnership%20Agreement%20was%20signed%20in%20October%202008.&text=makes%20it%20possible%20for%20CARIFORUM,integration%20and%20regional%20value%20chains [https://perma.cc/FY9R-89E5]. Other agreements merely recognize principles for the collection, processing and storage of personal data such as: prior consent, legitimacy, purpose, proportionality, quality, safety, responsibility and information, but without developing this in detail. *Argentina - Chile Free Trade Agreement*, UNCTAD INV. POL'Y HUB art. 11.2.5(f) n.1, https://investmentpolicy.unctad.org/international-investment-agreements/treaties/treaties-with-investment-provisions/3796/argentina---chile-fta-2017- [https://perma.cc/ZZC8-E7AS]; *Chile – Uruguay*

EU has also pushed for more safeguards, requiring its partners to adopt appropriate measures to ensure the privacy protection while allowing the free movement of data, establishing a criterion of "equivalence."[289] Parties also commit to inform each other of their applicable rules and negotiate reciprocal, general or specific agreements,[290] as exemplified by the additional adequacy decisions of the European Commission, most recently with Japan.[291] As noted above, the EU wishes to permit data flows only if coupled with the high data protection standards of the GDPR.[292] In its currently negotiated trade deals with Australia,[293] New Zealand,[294] and Tunisia,[295] as well as in the EU proposal for WTO rules

Economic Complementation Agreement No. 75, UNCTAD INV. POL'Y HUB, art. 8.2.5(f) n.3, https://investmentpolicy.unctad.org/international-investment-agreements/treaties/treaties-with-investment-provisions/3709/chile---uruguay-fta-2016- [https://perma.cc/88BS-WKWW].

289. *See Q&A, supra* note 261; *see also* U.N. Division on Technology and Logistics, *Data Protection Regulations and International Data Flows: Implications for Trade and Development*, UNCTAD/WEB/DTL/STICT/2016/1/iPub (2016).

290. *Free Trade Agreement Between the European Union and Singapore*, art. 8.54, ¶ 2, Nov. 14, 2011, O.J. (L 294); *Protocol on Mutual Administrative Assistance on Custom Matters*, art. 10, Oct. 21, 2016, O.J. (L 287); *Protocol 5 on Mutual Administrative Assistance on Custom Matters*, art. 10.2, Bosn. & Herz., Mar. 20, 2004, O.J. (L 84); *Euro-Mediterranean Agreement Establishing the European Community and its Member States, of the One Part, and the People's Democratic Republic of Algeria, of the other Part*, art. 45, Oct. 10, 2005, O.J. (L 265); *Euro-Mediterranean Agreement Establishing the European Community and its Member States, of the One Part, and the People's Democratic Republic of Algeria, of the other Part, Protocol No. 7*, Oct. 10, 2005, O.J. (L 265).

291. *See* 2019 O.J. (L 76).

292. *See Horizontal Provisions*, *supra* note 265, at art. A(1).

293. *See* European Union's Proposal for the EU-Australia Free Trade Agreement, EU-AUSTL., Oct. 10, 2018, https://trade.ec.europa.eu/doclib/docs/2018/december/tradoc_157570.pdf [https://perma.cc/GC44-HT6D].

294. *See* European Union's Proposal for the EU-New Zealand Free Trade Agreement, EU-N.Z., Sept. 25, 2018, https://trade.ec.europa.eu/doclib/docs/2018/december/tradoc_157581.pdf [https://perma.cc/9AZ7-2V5G].

295. *See* La Proposition de l'Union Européenne pour l'Accord de Libre-échange EU-Tunisie [The European Union's Proposal for the EU-Tunisia Free Trade Agreement], EU-Tunis., Nov. 8, 2018, https://trade.ec.europa.eu/doclib/docs/2019/january/tradoc_157660.%20ALECA%202019%20-%20texte%20commerce%20numerique.pdf [https://perma.cc/RH9G-CP7P].

on electronic commerce,[296] the EU follows a distinct model of endorsing and protecting privacy as a fundamental right.[297] On one hand, the EU and its partners seek to ban data localization measures and subscribe to a free data flow, but on the other hand, these commitments are conditioned. These conditions include first a dedicated article on data protection, which clearly states that "[e]ach Party recognizes 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,"[298] followed by a paragraph on data sovereignty, which states that, "[e]ach 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."[299] The EU also wishes to retain the right to see how the implementation of the FTA impacts the conditions of privacy protection specifically with regards to data flows.[300] In this sense, there is a review possibility within three years of the entry into force of the agreement and parties remain free to propose a review of the list of restrictions at any time.[301] In addition, there is a broad carve-out in the treaty stating that, "[t]he Parties reaffirm the right to regulate within their territories to achieve legitimate policy objectives, such as the protection of public health, social services, public education, safety, the environment including climate change, public morals, social or consumer protection, privacy and data protection, or the promotion and protection of cultural diversity."[302] The EU thus reserves ample regulatory leeway for its current and future data protection measures. The exception is also fundamentally different than the objective necessity test under the CPTPP and the USMCA, or that under WTO law, because it is subjective in nature and safeguards the

296. Communication from the European Union, *Joint Statement on Electronic Commerce, EU Proposal for WTO Disciplines and Commitments Relating to Electronic Commerce*, WTO Doc. INF/ECOM/22 (Apr. 26, 2019).

297. 2000 O.J. (C 364) 10, at art. 7.

298. *See, e.g.*, EU-Australia Free Trade Agreement, *supra* note 293 at art. 6(1); European Union's Proposal for the EU-New Zealand Free Trade Agreement, *supra* note 294; The European Union's Proposal for the EU-Tunisia Free Trade Agreement, *supra* note 295.

299. *See, e.g.*, EU-Australia Free Trade Agreement, *supra* note 293, at art. 6(2).

300. *Id.* at art. 5(2).

301. *Id.*

302. *Id.* at art. 2.

EU's right to regulate.[303] While the new EU approach has been confirmed by the recently adopted post-Brexit Trade and Cooperation Agreement ("TCA") with the United Kingdom,[304] the EU appears likely to tailor its template depending on the trade partner — for example, the negotiated agreement with Chile has, at least so far, no provisions on data flows and data protection,[305] while the negotiated deal with Indonesia includes merely a place-holder for rules on data flows.[306] The recently signed agreement with Vietnam, which entered into force on August 1, 2020, has only a few cooperation provisions on electronic commerce as part of the services chapter and does not refer to either data or privacy protection.[307] One should also be reminded that many agreements following the EU model, such as the draft e-commerce chapter of the countries of the European Free Trade Area ("EFTA"),[308] as well as the DEPA[309] include a general exception clause that follows the lines of Article XIV of the GATS to be applied *mutatis mutandis,* and permits exceptions across all sectors and on top of the mentioned carve-outs.[310]

An interesting and much anticipated development against the backdrop of the diverging EU and US positions has been the recent

303. Svetlana Yakovleva, *Privacy Protection(ism): The Latest Wave of Trade Constraints on Regulatory Autonomy*, 74 UNIV. MIA. L. REV. 416, 496 (2020).

304. 2020 O.J. (L 444) 14.

305. *European Union's Proposal for the EU-Chile Free Trade Agreement*, EUROPEAN COMMISSION, https://trade.ec.europa.eu/doclib/docs/2018/february/tradoc_156582.pdf [https://perma.cc/7285-TL96].

306. *European Union's Proposal for the EU-Indonesia FTA*, EUROPEAN COMMISSION, http://trade.ec.europa.eu/doclib/press/index.cfm?id=1620 [https://perma.cc/PN6F-5692].

307. *See* Free Trade Agreement Between the European Union and the Socialist Republic of Viet Nam, E.U.-Viet., Dec. 6, 2020, O.J. (L 186).

308. The EFTA countries are Lichtenstein, Norway, Switzerland and Iceland. They have so far not included any e-commerce provisions in their FTAs, as a group or separately, except for the Japan-Switzerland FTA of 2009, which has some, mostly non-binding provisions on digital trade. The author has consulted the EFTA Advisory Committees on the draft EFTA e-commerce chapter and has the text on file. *See About EFTA*, EUROPEAN FREE TRADE ASS'N, https://www.efta.int/about-efta [https://perma.cc/M5WS-ZY7G].

309. *The Digital Economy Partnership Agreement (DEPA)*, MINISTRY OF TRADE AND INDUSTRY SING., Sing.-Chile-N.Z., art. 13.1, June 12, 2020 [hereinafter DEPA], https://www.mti.gov.sg/-/media/MTI/Microsites/DEAs/Digital-Economy-Partnership-Agreement/Text-of-the-DEPA.pdf [https://perma.cc/HN3B-C87K].

310. It is often the case that there are sectorial carve-outs too that this article does not elaborate upon – for instance, in the areas of audiovisual and financial services, as well as government procurement.

Regional Comprehensive Economic Partnership ("RCEP") between the ASEAN Members,[311] China, Japan, South Korea, Australia, and New Zealand. In terms of norms for the data-driven economy, the RCEP is certainly a less ambitious effort than the CPTPP and the USMCA, but still brings about significant changes to the regulatory environment and, in particular, to China's commitments in the area of digital trade. The RCEP provides only for conditional data flows while preserving a lot of policy space for domestic policies, which very well may be of a data-protectionist nature. So, while the RCEP e-commerce includes a ban on localization measures,[312] as well as a commitment to free data flows,[313] there are clarifications that give RCEP members significant policy space and essentially undermine the impact of the existing commitments. In this line, there is an exception possible for legitimate public policies and a footnote to Article 12.14.3(a), which says that, "[f]or the purposes of this subparagraph, the Parties affirm that the *necessity* behind the implementation of such legitimate public policy *shall be decided* by the implementing Party." This essentially goes against any exceptions assessment as we know it under WTO law and triggers a self-judging mechanism. In addition, subparagraph (b) of 12.14.3 says that the article does not prevent a party from taking "any measure that it considers necessary for the protection of its *essential security interests*."[314] Such measures shall not be disputed by other Parties.[315] Article 12.15 on cross-border transfer of information follows the same language and thus secures plenty of policy space, for countries like China or Vietnam, to control data flows without further justification.[316]

311. Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, Philippines, Singapore, Thailand and Vietnam. *What is ASEAN?*, COUNCIL ON FOREIGN RELATIONS (2020), https://www.cfr.org/backgrounder/what-asean#:~:text=The%20Association%20of%20Southeast%20Asian%20Nations%20(ASEAN)%20is%20a%20regional,Singapore%2C%20Thailand%2C%20and%20Vietnam [https://perma.cc/KT2U-5LNJ].

312. *Regional Comprehensive Economic Partnership*, art. 12.14 (2020), https://www.dfat.gov.au/trade/agreements/not-yet-in-force/rcep/rcep-text-and-associated-documents [https://perma.cc/V87Q-LWMA].

313. *Id.* at art. 12.15.

314. *Id.* at art. 12.14.3(b) (emphasis added). The "essential security interest" language has been endorsed by China also in the framework of the WTO e-commerce negotiations. *See* WTO Electronic Commerce Negotiations, *Consolidated Negotiating Text*, WTO Doc. INF/ECOM/62/Rev. 1 (Dec. 14, 2020).

315. *Id.* at art. 12.14.3(b)

316. *Id.* at art. 12.15.3 (a) & (b).

E. PROS AND CONS OF THE EXISTING RECONCILIATION MODELS

The above sections revealed not only the intensified contestation between free data flows as an essential element of the data-driven economy and the protection of privacy as a sovereign right of states to safeguard their citizens, but also the different regulatory approaches states have sought to reconcile these interests. In the face of failing international cooperation and the diverging positions of the major stakeholders of the EU and the US, trade venues, and perhaps oddly — or even wrongly so —[317] have become platforms for rule-creation that try to interface data flows and privacy protection. However, we are far from an optimal model. States are still grappling to find viable mechanisms, which not only provide a level of certainty and market access for businesses but also reflect the state's societal values.

Each of the existing models comes with certain pros and cons. The international framework is not fully developed with regard to privacy protection; it is not binding, nor does it have mechanisms that can effectively reconcile the clash of rights.[318] The transnational regimes under the OECD and the APEC, though still not binding and of club-nature, have provided agreement on some basic regulatory principles that shape domestic frameworks, while at the same time ensure the free flow of information.[319] As the underlying principles of these frameworks become increasingly integrated into trade law, which enhances their regulatory strength and diffusion across countries, they may provide a good way to tackle the tensions. However, oversight and enforceability in the case of violations remain important questions without an adequate answer. For countries, like the EU Member States, that demand appropriate checks and balances for the protection of individual rights, they may, plainly, not be enough. In the area of international trade law, we have the generic exception clauses under Article XX of the GATT and Article XIV of the GATS.[320] Similar clauses have also been replicated in a number of FTAs *mutatis mutandis*.[321] They provide for a stringent test that seeks to constrain protectionism when states pursue non-economic objectives; but since

317. *See* Yakovleva, *supra* note 303, at 497.

318. *See generally* Yakovleva & Irion, *supra* note 46.

319. *See About APEC*, ASIA-PACIFIC ECONOMIC COOPERATION, https://www.apec.org/About-Us/About-APEC [https://perma.cc/MT9W-NYKL]; *About*, ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, https://www.oecd.org/about/ [https://perma.cc/CGB9-ACZP].

320. GATT 1994, *supra* note 183, art. XX; GATS, *supra* note 184, art. XIV.

321. *See e.g.*, DEPA, *supra* note 309.

we have no jurisprudence,[322] we are yet unsure how they will be applied in practice, and whether for instance the EU's GDPR will not be found in violation of the EU's commitments under the GATS. It is also questionable whether an *ex post*, timewise protracted, case-by-case examination of alleged infringements can match the fluidity of the digital economy and the high stakes that are at hand. The CPTPP and the USMCA templates are modeled along the WTO norms but are linked to an even higher degree of uncertainty, as the legitimate objectives are not clearly spelled out. Coupled with the low privacy protection guarantees that these treaties provide, there seems to be a priority given to economic rights.[323] Such a stance, although it may make economic sense and boost growth and innovation, may be unacceptable for some actors, such as the EU, which places a high value on fundamental rights and seeks to ensure their effective protection.[324] The EU has accordingly sought to export its high standards of protection through an extension of the territorial application of the GDPR and unilateral adequacy decisions that, short of international harmonization, provide an adequate level of protection of the EU citizens' data.[325] This unilateral approach, while justified on the side of the EU, may be linked to higher costs of compliance for foreign firms and countries, and may have negative implications for the EU's economy and innovation capabilities in the era of Big Data and AI. One ingenious hybrid solution discussed above was the EU-US Privacy Shield as a flexible mechanism that reconciles the high standards of protection in the EU and the fairly low and fragmented levels of personal data protection in the US.[326] The EU-US Privacy Shield is by no means perfect, as it fails to satisfy high demands of bindingness and enforceability and does not live up to the level of protection that the EU wishes to provide for its citizens, as confirmed by the *Schrems* judgments.[327] However, the model has certain advantages: for example, there are working supervisory and remedy mechanisms, at least post-*Schrems I*, and potentially now moving towards an enhanced agreement post-*Schrems II*. Moreover, under such an agreement, the EU does not require firms to establish a costly presence in the EU, and the assessment of conformity with the EU standards takes place at home by domestic regulators.[328] It may thus be worthwhile to contemplate to

322. *See e.g.*, *id.*

323. *Id.*

324. European Parliament, *The Protection of Fundamental Rights in the EU*, FACT SHEETS ON THE EUROPEAN UNION (2020).

325. GDPR, *supra* note 31, at art. 45.

326. Downes, *supra* note 129.

327. *Id.*

328. *See id.*

what extent such or similar mechanisms may be shaped in a more binding treaty form, which will provide legal certainty,[329] and whether and how such mechanisms may be extended and made viable in plurilateral or multilateral contexts.[330] While the current negotiations on electronic commerce under the auspices of the WTO reveal at this stage little agreement and willingness to move forward,[331] preferential trade venues can serve as governance laboratories and pave the way towards regulatory cooperation and the possible implementation of the Privacy Shield model. Interoperability mechanisms can serve the data-driven economy better than a multitude of carve-outs and exceptions.

F. CONCLUDING REMARKS: THE PRESENT AND FUTURE OF THE TRADE AND PRIVACY INTERFACE

The contention between privacy and trade is by no means trivial, as on the one hand, fundamental individual rights and a nation's informational sovereignty are at stake, while on the other hand, the present and the future of a data-driven economy bringing multiple benefits to societies needs to be considered. Ideally, one might think that a substantive harmonization of levels of protection would be the way to go and both scholars[332] and policymakers[333] have contemplated this path. Joel Reidenberger has in particular suggested that the harmonization of data protection laws can be based on the model of the

329. Such a treaty could have superior legal force to EU regulations, such as the GDPR, but the defence through it the primary sources of EU law, such as the Charter of Fundamental Rights, remains. *See* CONG. RSCH. SERV., *supra* note 171, at 13.

330. *See generally* Aaditya Mattoo & Joshua P. Meltzer, *Data Flows and Privacy: The Conflict and Its Resolution*, 21 J. INT'L ECON. L. 769 (2018).

331. *See, e.g.*, Ines Willemyns, *Agreement Forthcoming? A Comparison of EU, US, and Chinese RTAs in Times of Plurilateral E-Commerce Negotiations*, 23 J. INT'L ECON. L. 221 (2020); Mira Burri, *Towards a New Treaty on Digital Trade*, 55 J. WORLD TRADE 71 (2021).

332. *See, e.g.*, David Cole & Federico Fabbrini, *Bridging the Transatlantic Divide? The US, the EU, and the Protection of Privacy Across Borders*, 14 INT'L J. CONST. L. 220 (2016); David Cole & Federico Fabbrini, *Transatlantic Negotiations for Transatlantic Rights: Why an EU-US Agreement Is the Best Option for Protecting Privacy against Cross-Border Surveillance*, *in* SURVEILLANCE, PRIVACY & TRANSATLANTIC RELATIONS (David Cole et al. eds., 2017); Ian Brown, *The Feasibility of Transatlantic Privacy-Protective Standards for Surveillance*, 23 INT'L J. L. INFO. TECH. 23 (2015).

333. *See, e.g.*, Cannataci, *supra* note 58; *see also Montreux Declaration: The Protection of Personal Data and Privacy in a Globalized World: a Universal Right Respecting Diversities* (Sept. 16,2005), http://globalprivacyassembly.org/wp-content/uploads/2015/02/Montreux-Declaration.pdf [https://perma.cc/ZA3J-4S5G].

WTO and move towards a General Agreement on Information Privacy;[334] yet, looking at the current state of affairs at the WTO, despite the invigoration of e-commerce dedicated talks, such a proposal does not seem feasible.[335] Some have also voiced concerns about perils along this path in case of an international accord, which might tilt heavily in favor of security-service preferences and in fact weaken privacy protection worldwide, so that "global privacy is likely to be better protected if domestic surveillance laws, especially those of the United States, are left to evolve on their own terms, without resort to a comprehensive multilateral framework."[336] Indeed, the reality of rule-making on the interface of trade and privacy appears somewhat different than as previously perceived. We are faced with two realities: First, and something that is rather unspectacular in the area of cyberlaw, it appears, as it was prophesied early on, that while potentially "many aspects of the Net will be governed on a global scale,"[337] "many Internet controversies are fast transforming into disputes among nations, and classic problems of international relations," where "governments fight . . . one another to favor themselves, using the traditional tools of international politics and international law."[338] Second, and this is a reality that this article has made apparent, trade law, in particular deals struck in preferential venues, has become the plane where the contention of trade and privacy protection plays out and becomes gradually regulated. However, the direction that this regulation will take is uncertain, as we appear somewhat stuck between the diverging positions of the two main legal entrepreneurs — the US and the EU, as well as the highly protective stance of China. The question then is who will dominate, or rather, are we faced with a situation where despite the differences we will have more common themes across jurisdictions in due time. Here again, opinions differ. While many have argued that the "Brussels effect" is occurring and the EU is ratcheting up US domestic standards of protection,[339] some have pointed to a more nuanced two-way relationship,[340] which seems to inform both legal orders, actors'

334. *See* Reidenberg, *supra* note 137, at 1360.

335. *See generally* Burri, *Towards a New Treaty on Digital Trade*, *supra* note 331.

336. Stephen J. Schulhofer, *An International Right to Privacy? Be Careful What You Wish For* (N.Y.U. Sch. L. Pub. L. Legal Theory Rsch. Paper Series 27, Working Paper No. 15-15, 2015).

337. JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET?: ILLUSIONS OF A BORDERLESS WORLD, 164 (2008).

338. *Id.*

339. *See* Bradford, *supra* note 286, at 3–6; Shaffer, *supra* note 9, at 2–3.

340. Shaffer, *supra* note 9, at 6.

positioning, and enhance rule-diffusion.[341] While a final statement on these diverging directions is still out, it appears clear and beneficial that levels of international cooperation are to be fostered, even through second-best mutual recognition solutions, such as the Privacy Shield Framework, which should not be perceived as weakening the sovereign state but rather as a logical response to the increased interdependence resulting from globalization and the spread of new communication technologies.[342]

To conclude, one can underscore that privacy protection has clearly become a key topic on the trade negotiation tables and there is new and evolving rule-making that seeks to interface the demands of the digital economy to permit free flowing data and the sovereign wish to adequately safeguard the rights and values embedded in individual societies.[343] Trade policy has the capacity to promote trade and innovation despite varying standards for privacy protection, but there is a strong demand for enhanced regulatory cooperation.[344] As the complexity of the data-driven society rises, regulatory cooperation seems indispensable moving forward, since data issues cannot be addressed by the plain "lower tariffs, more commitments" stance in trade negotiations but instead demand effective reconciliation mechanisms and continuous oversight.[345] At the same time, it appears that there will not be an "one-size-fits-all" solution, but rather a complex and conflicted regulatory environment that will continue to evolve.[346]

---

341. *See, e.g.*, Bilyana Petkova, *Domesticating the "Foreign" in Making Transatlantic Data Privacy Law*, 15 INT'L J. CONST. L. 1135 (2018).

342. Henry Farrell, *Hybrid Institutions and the Law: Outlaw Arrangements or Interface Solutions?*, 23 ZEITSCHRIFT FÜR RECHTSSOZIOLOGIE 25, 26 (2002).

343. U.N. Conf. on Trade and Dev., *Digital Economy Report 2019*, UNCTAD/DER/2019 (2019).

344. Thomas J. Bollyky & Petros C. Mavroidis, *Trade, Social Preferences, and Regulatory Cooperation: The New WTO-Think*, 20 J. INT'L ECON. L. 1, 11 (2017) (discussing the need for regulatory competition in the context of global value chains; the argument is only strengthened in the domain of digital trade); *see also* Usman Ahmed, *The Importance of Cross-Border Regulatory Cooperation in the Era of Digital Trade*, 18 WORLD TRADE REV. s99 (2019).

345. *See, e.g.*, Thomas Cottier, *International Economic Law in Transition from Trade Liberalization to Trade Regulation*, 17 J. INT'L ECON. L. 671, 672 (2014).

346. *See, e.g.*, Henry Farrell and Abraham L. Newman, *The Janus Face of the Liberal International Information Order: When Global Institutions Are Self-Undermining*, 75 INT'L ORG. 1 (2021).